Information Technology Master Plan

Version 5.7

Rogue Community College

Document Details

Document Title	**Information Technology Master Plan**
Document Type	Operational Plan
Document ID	Rogue Community College -ITM-01
Classification	Internal
Distribution	All
Effective Date	

Version Control

Version	Date	Author	Description
1.0	May 2023	Jeremy Taylor	Original Document Creation
2.0	August 2023	Lisa Stanton	Document review and modification suggestions
3.0	November 2023	Jeremy Taylor	Modifications and edits
4.0	February 2024	Lisa Stanton	Final Review
5.0	June 2024	Jeremy Taylor	P&P Committee Work and review
5.5	August 2024	Jeremy Taylor, Jamee Harrington, Steven Phelps, Sean Taggart	Committee Work

5.7	November 2024	Jeremy Taylor	Modifications and edits recommended by Executive Team

Approvals

Name	Title	Signature	Date
	Chief Information Officer		
Lisa Stanton	Vice President/Chief Financial Officer		
Anupendu Ghosh	Director of IT		

TABLE OF CONTENTS

EXECUTIVE SUMMARY

OVERVIEW

The Information Technology (IT) Master Plan is essential for guiding Rogue Community College (RCC) in achieving its strategic goals. It aligns technology initiatives with the college's broader mission, providing a comprehensive roadmap for technology strategy development, procurement, replacement, and deployment across the district. This alignment underscores the vital role of technology in enhancing academic excellence, operational efficiency, and community engagement—core elements of the College's mission.

By clearly articulating the district's technological mission, the IT Master Plan outlines specific technology goals and objectives that closely align with RCC's overall strategic ambitions. This alignment underscores the vital role of technology in enhancing academic excellence, operational efficiency, and community engagement—core elements of the College's mission.

A central feature of this plan is the establishment of strong technology standards and clear criteria for acquiring new technology. These standards ensure consistency, security, and interoperability, while the acquisition criteria emphasize value, effectiveness, and alignment with RCC's mission.

Regular refresh cycles for equipment are established to maintain a robust technological infrastructure. These cycles, influenced by technological advancements, budget considerations, and institutional needs, ensure RCC remains current with evolving technology.

The IT department plays a critical role in planning, managing, and leading technology initiatives, supporting academic and administrative functions at RCC by developing, monitoring, and maintaining the campus data network, telephone system, computer systems and servers, computer labs, smart classrooms, and conference rooms. This ensures a supportive technology environment for learning, collaboration, and administration.

The effectiveness and funding of the initiatives in this plan will be evaluated annually based on institutional needs and available resources. Stakeholder engagement is crucial in creating and evolving the plan, ensuring it remains responsive, relevant, and aligned with RCC's educational and operational goals. A governance structure will oversee the implementation of the IT Master Plan, ensuring financial prudence and alignment with RCC's strategic priorities.

The IT Master Plan is a dynamic document, evolving with new technology trends, innovations, and the changing needs of the RCC community. Stakeholder engagement is crucial in creating and evolving the plan, ensuring it remains responsive, relevant, and aligned with RCC's educational and operational goals.

This document is structured to provide a clear progression from general concepts to specific strategies, action plans, and evaluation metrics, supporting the successful execution and assessment of the IT Master Plan.

INTRODUCTION

IT MISSION

The mission of the Information Technology (IT) department at Rogue Community College (RCC) is to create an environment where every student and staff member has easy access to essential technology resources and information. The primary goal is to provide an efficient, intuitive, and user-friendly technological infrastructure that supports academic and administrative activities.

Key aspects of this mission include delivering a secure, reliable, and cost-effective technology framework that ensures smooth daily operations. To achieve this, the department focuses on the following key areas:

1. **Digital Inclusivity**:
   Ensuring that everyone in the community, regardless of technical skills, can access and use the necessary technological tools and resources for academic or administrative work.

2. **Operational Efficiency**:
   Committing to continuous improvement in operations to enhance user experience, reduce downtime, and increase overall productivity.

3. **Security and Reliability**:
   Adhering to strict measures to protect sensitive data and ensure system reliability, thereby building trust in the technology services provided.

4. **Cost-Effectiveness**:
   Managing resources wisely to deliver top-quality services at the lowest possible cost, maximizing the value of technology investments.

5. **Strategic Alignment**:
   Ensuring all technology initiatives support and contribute to the College's Strategic Plan.

6. **Software Uniformity**:
   Promoting standardized software applications across the institution to ensure consistency, ease of use, and data integrity. This approach aims to eliminate data redundancy and improve operational efficiency.

Focusing on these areas will create a technological environment that enables every member of the RCC community to succeed in their roles, bringing the College closer to its strategic goals.

STRATEGIC INITIATIVES

The IT Master Plan outlines a comprehensive strategy to enhance and maintain Rogue Community College's (RCC) technology use, aiming to protect the College's investment in technology through careful planning and smart management. This plan serves as a guide for managing RCC's technology assets, from phasing out outdated hardware to adopting new software, setting up smart classrooms, meeting growing network demands, and identifying evolving instructional needs.

The main goals and scope of the IT Master Plan include:

1. **Flexibility**:
   The plan is designed to adapt to the rapidly changing world of technology. As new technologies emerge and existing ones evolve, the plan facilitates their integration to best serve the RCC community.

2. **Collaborative Decision-Making**:
   The plan encourages broad participation in decision-making and technology acquisition, ensuring that investments and initiatives meet the diverse needs and perspectives of the RCC community.

3. **Adaptability**:
   Given the fast-paced changes in technology and community needs, the plan is built to accommodate these shifts, keeping RCC at the forefront of technological innovation and enabling quick responses to new challenges or opportunities.

4. **Asset Management**:
   The plan outlines a structured approach for managing RCC's technology assets annually. By carefully tracking and planning for the replacement and addition of hardware and software, the plan aims to optimize the use and extend the lifespan of technology investments.

5. **Network Demand Management**:
   As network demands increase, the plan empowers RCC to manage these pressures proactively, ensuring consistent digital service performance.

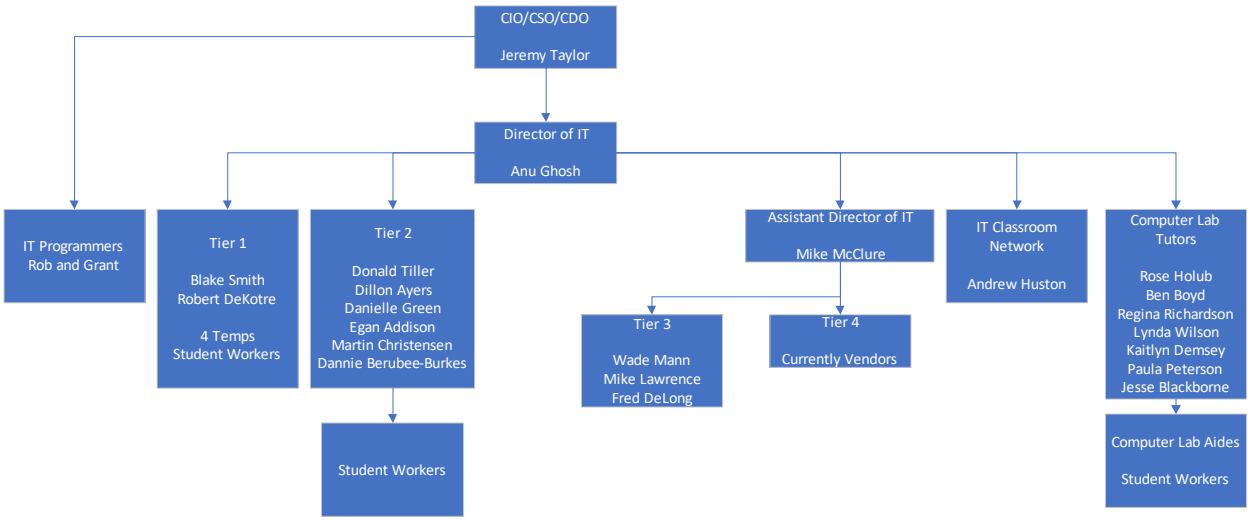
6. **Instructional Needs Identification**:
   The plan includes a proactive approach to identifying and addressing the technological

requirements of instructional design, ensuring that the most effective tools support teaching and learning environments.

Through these strategic initiatives, the plan aims to create a technologically advanced, responsive, and inclusive environment that fully supports the needs and aspirations of the RCC community.

ORGANIZATION CHART

The current vision for a new tier system to IT staffing:



OBJECTIVES

The primary objectives of the RCC Information Technology (IT) department are:

1. **Technology Infrastructure Management**:
   Maintaining and supporting the college's technology infrastructure, including hardware, software, and network systems, to ensure resilience, reliability, and alignment with the institution's needs.

2. **Data Security and Privacy**:
   Protecting sensitive data and systems is a top priority. The department implements the latest security measures to safeguard the community's information from potential threats.

3. **Data Management Systems**:
   Establishing and maintaining efficient systems for data storage, retrieval, and analysis, ensuring that critical information is easily accessible and secure.

4. **Technical Support**:
   Providing ongoing technical support to staff, faculty, and students, resolving issues promptly to minimize disruptions and enhance the user experience.

5. **Technological Efficiency**:
   Utilizing technology effectively and efficiently to support the college's goals, boost productivity, encourage innovation, and promote academic excellence.

6. **Technology Trend Awareness**:
   Staying updated on technology trends and innovations, evaluating their potential benefits for the college, and recommending new technologies to improve efficiency and effectiveness.

7. **Technology Project Management**:
   Managing and implementing technology projects, including upgrades, migrations, and installations, ensuring they are completed on time, within budget, and with minimal disruption.

8. **Manuals, Guidelines, and Procedure Development**:
   Developing and maintaining manuals, guidelines, and procedures to guide technology use within the college, ensuring compliance with regulations, promoting best practices, and fostering responsible technology use.

9. **Cross-Departmental Collaboration**:
   Collaborating with other departments and teams to ensure that technology effectively supports the college's goals, aligning tech initiatives with RCC's broader strategic objectives.

10. **IT Budget Management**:
    Managing the IT budget effectively, ensuring that technology investments align with the college's financial goals while balancing cost-effectiveness with quality and innovation.

Through these objectives, the IT department seeks to create a technologically advanced and secure environment that fully supports the needs and aspirations of the RCC community.

GOALS AND OBJECTIVES 2024-2027

LONG-TERM IT GOAL 1: ENHANCING ACCESSIBILITY AND SUPPORT

Department Goal:
Develop and maintain advanced, accessible IT support systems and services to enhance the user experience for all stakeholders.

Rationale:
The rationale for enhancing IT accessibility and support is deeply rooted in college and divisional goals. By focusing on accessibility, the IT department aligns with the college's core values of diversity, equity, and inclusion, ensuring all college community members have equitable access to IT resources. This goal also ties into the divisional objective of providing consistent, accurate, and timely support services, as improved accessibility naturally leads to increased efficiency and user satisfaction. It supports the college's vision of being an inclusive and dynamic institution that empowers student success and economic development by providing exemplary educational opportunities through robust IT support.

Key Objectives:

2024 Objectives:

- Survey users, targeting a response rate of at least 60%, to identify current accessibility challenges within IT support.
- Benchmark IT systems against international accessibility standards like WCAG 2.1, aiming for at least 75% compliance. Add a piece to look at all software owned by the college.
- Document the current state of IT support tools, setting a baseline for future comparison.
- All staff training on IT Help Me Portal and form usage.

2025 Objectives:

- Evaluate the effectiveness of our current IT support portal to increase user satisfaction ratings by 25%.
- Implement a feedback mechanism to gather ongoing insights, aiming for at least 100 unique user interactions per month.
- Develop educational materials on new portal features and distribute them to IT support users.

2026 Objectives:

- Launch AI chatbots to reduce average query response time by 30%.
- Create a self-help resource library and track usage, aiming to reduce basic support tickets by 30%.
- Integrate the portal with other college systems, ensuring a seamless user experience across 60% of platforms.

2027 Objectives:

- Form a user experience focus group with diverse representation from all college sectors.
- Utilize user interaction analytics to refine tools and resources, aiming for a 20% improvement in user interaction scores.
- Schedule and execute bi-annual upgrades to the support portal, with each upgrade based on at least three key user feedback points.

Resource Allocation:
Outline the staffing, technology, and budgetary resources needed for each objective, ensuring that plans are grounded in available resources.

LONG-TERM IT GOAL 2: STRENGTHENING CYBERSECURITY AND INCIDENT RESPONSE

Department Goal:
Establish a robust cybersecurity posture with proactive threat identification and a comprehensive incident response strategy.

Rationale:
Strengthening cybersecurity and incident response prepares Rogue Community College to handle modern cyber threats proactively, supporting the college's core value of integrity by protecting sensitive data and systems. This goal directly responds to the divisional goal of building resilient infrastructures, ensuring that IT systems are robust, secure, and prepared for potential incidents. It supports the college's vision by fostering a safe and secure learning environment, thus contributing to a transformative educational experience. Furthermore, it emphasizes collaboration by involving multiple departments in cybersecurity efforts, enhancing communication and cooperation across divisions.

Key Objectives:

2024 Objectives:

- Conduct a detailed cybersecurity risk assessment, aiming for a 30% reduction in identified vulnerabilities over the 2021 Eide Bailly Cybersecurity Risk Assessment.

- Implement a mandatory cybersecurity training initiative, ensuring all IT personnel complete a program of their choice, subject to approval.
- Develop an Incident Response Plan framework and set up a response team with quarterly reviews.

2025 Objectives:

- Conduct biannual cyber-attack simulations to test and refine the Incident Response Plan.
- Enhance the cybersecurity training program with at least two interactive scenario-based activities.
- Deploy real-time monitoring and establish a cybersecurity incident dashboard, aiming for a 25% faster threat detection rate.

2026 Objectives:

- Integrate advanced threat detection tools, aiming for a detection accuracy of over 90%.
- Establish a cybersecurity operations center or partner with a third-party service.
- Update the Incident Response Plan to address the latest cyber threats with semi-annual revisions.

2027 Objectives:

- Review and update cybersecurity policies annually, ensuring alignment with current threats and regulations.
- Conduct bi-annual cyber incident response drills, aiming for a 20% improvement in response time with each drill.
- Engage with the cybersecurity community quarterly to stay abreast of emerging trends and defense strategies.

Stakeholder Engagement:

Outline a plan for regular collaboration and communication with key college departments and stakeholders to ensure an integrated approach to cybersecurity.

LONG-TERM IT GOAL 3: ITERATIVE DEVELOPMENT OF IT MASTER PLAN

Department Goal:
Continuously evolve the IT Master Plan to guide strategic IT initiatives, ensuring alignment with institutional goals and compliance requirements.

Rationale:
The iterative development of the IT Master Plan ensures that the IT department's strategies remain aligned with RCC's evolving strategic plan, particularly the Wildly Important Goals of Institutional Excellence. By continually updating the Master Plan, the IT department underscores its commitment to continuous improvement, a core college value. This ongoing process ties directly to the divisional goal of incorporating sustainable policies and procedures by ensuring that IT strategies remain relevant and forward-thinking. It also supports the college's objectives of leveraging technology to improve operational efficiency and student experiences by proactively addressing audit and compliance standards, including GLBA requirements, reflecting the college's vision for dynamic and responsive governance.

Key Objectives:

2024 Objectives:

1. Finalize and publish the initial version of the IT Master Plan, ensuring it aligns with current institutional goals and compliance requirements.
2. Conduct a review of the IT infrastructure and systems against the initial draft of the Master Plan, identifying gaps and areas for improvement.

2025 Objectives:

1. Implement the first phase of strategic initiatives identified in the Master Plan, focusing on critical areas such as cybersecurity, data management, and user experience.
2. Establish a formal feedback mechanism for collecting input from various stakeholders on the Master Plan's effectiveness and areas for refinement.

2026 Objectives:

1. Revise and update the IT Master Plan based on the feedback received and the progress of implemented initiatives, incorporating emerging technology trends and institutional changes.
2. Launch a series of targeted professional development programs for IT staff to align skills and expertise with the evolving needs of the IT Master Plan.

2027 Objectives:

1. Develop a sustainable model for the continuous evolution of the IT Master Plan, incorporating agile methodologies and regular stakeholder engagement.
2. Initiate a comprehensive evaluation of the Master Plan's impact on the institution's overall technological advancement and operational efficiency.

In achieving these objectives, the IT department commits to a balanced approach that prioritizes strategic resource allocation and active stakeholder engagement. This dual focus ensures that the IT Master Plan aligns with Rogue Community College's evolving needs and leverages its diverse community's insights and contributions. Through this approach, we aim to foster a technologically advanced, efficient, and collaborative IT environment that supports and amplifies the college's broader mission and goals.

SCOPE OF SUPPORT

The RCC IT Department is committed to protecting users and equipment from unauthorized or harmful actions. This manual outlines the acceptable use of the College's IT resources, and all staff members must ensure their use aligns with the guidelines provided, staying within authorized parameters for access, use, distribution, and modification.

This manual is central to the IT Department's policies and procedures, applying to all IT resources owned or leased by the College, including, but not limited to, computer equipment, software, operating systems, storage media, and internet access. These guidelines may also extend to privately-owned equipment connected to the College's network.

Users of IT resources are required to follow all College policies and manuals, including the Employee Resource Guide and this manual, while also complying with local, state, and federal laws and regulations. Non-compliance may result in disciplinary action, legal measures, or other appropriate remedies as determined by the College. Adherence to laws such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) is essential.

Other administrative units within the College may develop additional policies and procedures related to IT resource use; however, these must align with this manual and other relevant technology-related policies.

This manual aims to create a secure and orderly environment for using IT resources, encouraging responsible digital behavior among users while ensuring the College's IT assets are

used appropriately to support the institutional mission and goals. Clear expectations and consequences are set to maintain a respectful, productive, and legally compliant digital environment.

FUNDING AND BUDGET PROCESS

Successfully implementing the Information Technology Master Plan depends on securing sufficient funding. Without the necessary funds to update the Technology Replacement component, the plan risks becoming outdated within a year. For the 2024/2025 academic year, the Technology Fee and the College Service Fee will be merged into a single Universal Fee, providing IT with more flexible funding.

When budgeting for new technology, it is crucial to consider the total cost of ownership. This includes factors such as equipment aging, expiring warranties, repair and maintenance costs, recurring licensing fees, and other related expenses. The Information Technology Master Plan promotes a comprehensive and sustainable strategy, aiming to prevent last-minute or reactive management through annual reviews.

The updated timeline and process for developing the IT budget are as follows:

- **December**:
  IT reviews the Five-Year Spending Plan to ensure current items are up-to-date and identifies new Technology Replacement needs for the next academic year.
- **January**:
  IT builds budgets using college-approved software, creating new ActionPaks. The Vice President of Operations and Finance reviews and approves the budget, which is then shared with the Executive Team for their review and approval. The Technology Replacement needs budget is also shared with the Budget Advisory Team for review.
- **April**:
  The executive team reviews Budgets and ActionPaks and finalizes them for submission to the Budget Committee for review and approval.
- **May**:
  The Budget Committee approves and prepares the budget for Board approval.
- **June**:
  The Board of Education approves the final budget, including Technology Replacement needs.

In addition to the general fund budget, other potential funding sources for technology include grants, capital project funds from new construction or major remodels, and donations. These

additional funding sources provide greater flexibility and sustainability for the college's technology investments.

PLANNING

Effective information technology planning at Rogue Community College (RCC) aims to align institutional priorities with technological objectives. This strategic planning process helps assess the current state, envision the future, and determine how technology can best support the College's goals.

Technology projects should be integrated into the broader college planning process to ensure a unified approach. Planning technology projects that align with the goals of specific departments, administrative units, or the entire institution should be coordinated with the relevant entities.

Key components of this planning process include:

1. **Identifying Needs and Outcomes**:
   Every project should have a clearly defined need and desired outcome documented for future reference.
2. **Consolidation of Projects**:
   Projects with similar goals should be grouped to optimize resource use.
3. **User Consultation**:
   End users or their representatives should be consulted before finalizing the planning process. Their feedback is invaluable and should be prioritized to ensure the technology effectively meets their needs.
4. **Ensuring User Utility**:
   Any technological improvements that might negatively affect users should include a detailed plan to restore or exceed the previous level of utility within a reasonable timeframe.

The planning process aligns with a broader planning framework that ensures:

- The plan matches RCC’s vision, mission, and goals.
- The plan facilitates knowledge sharing about technological needs and limitations.
- The plan addresses key institutional, academic, and community needs through technology.

To align with the college's priorities, various planning documents are referenced, including:

- Rogue Community College Strategic Plan

- Annual Program Review Updates
- Academic Master Plan
- Facilities Master Plan

A Five-Year Spending Plan is also created and maintained to ensure preparedness for long-term technology investments and replacements. This plan is reviewed annually to adjust for changes in technology needs, budget constraints, or institutional priorities.

Beyond the annual program review process, new projects may arise throughout the year as opportunities emerge. The "Request Form for Technology Projects" has been created to help identify and communicate technology projects' full scope and total cost. The timing of project implementation will be decided annually based on college priorities, department functionality, and the availability of funding and staffing resources.

Information Technology Guidelines Handbook

Rogue Community College

GUIDELINES AND PROCEDURES AMENDMENT PROCESS

Overview:

Rogue Community College (RCC) follows a structured process for amending its IT Manuals and Procedures, aligning with the college-wide policy and procedure amendment processes outlined in BP 2410 (Board of Education Policies and Administrative Procedures) and AP 2410 (Board Policies and Administrative Procedures). This process aims to maintain the relevance and effectiveness of IT policies and procedures while ensuring a fair and transparent approach to any amendments.

Guidelines:

1. **Initiation of Amendment:**
   Amendments to the IT Master Plan can be initiated by the Chief Information Officer (CIO) or as part of the college-wide policy and procedure amendment process outlined in BP 2410 and AP 2410.
2. **Submission of Change Request:**
   Staff members with suggestions for amendments are encouraged to communicate these to their immediate supervisors or directly to the CIO. Formal change requests will be processed according to the college-wide amendment process.
3. **Review of Change Request:**
   Upon receipt of a change request, the CIO will review it in alignment with AP 2410, ensuring adherence to the broader institutional policy amendment framework.
4. **Development of Action Plan:**
   If the change request merits further review, the IT Department or the relevant committee will develop an action plan following the processes outlined in AP 2410.
5. **Approval:**
   Significant amendments to the IT Master Plan will be presented to the College Leadership Team for approval, following BP 2410 and AP 2410 guidelines.
6. **Communication of Amendments:**
   Once approved, the CIO will communicate any amendments to IT Policies and Procedures to college staff and faculty, ensuring they are informed before the changes take effect.
7. **Implementation:**
   The IT Department will implement the amendments according to the approved action plan and within the broader institutional policy amendment process framework.

This amendment process ensures that RCC's IT policies and procedures remain current, aligning with the broader institutional framework for policy and procedure amendments. It also aims to balance the need for policy evolution with the practical considerations of managing change within the IT Department.

ACCEPTABLE USE POLICY

The college has a formal policy and subsequent procedure adopted for acceptable use guidelines, which can be found here:

BP-3720 (Computer and Network Use) AP-3720 (Computer and Network Use)

These documents provide the rules and regulations for using the college's technology equipment. It applies to all College staff and faculty, volunteers, and students.

ACCESSIBILITY POLICY

Overview:

Rogue Community College (RCC) is committed to providing equal access to information for students, faculty, staff, and the community, including individuals with disabilities, as defined by Section 504 of the Rehabilitation Act of 1973 (as amended), Section 508, and the Americans with Disabilities Act of 1990 (ADA, as amended). RCC strives to proactively identify and remove barriers, ensuring access to its programs, services, and activities.

This policy establishes specific standards for the IT Accessibility Policy (ITAP) to ensure compliance with applicable accreditation, federal regulations, and laws. Operational procedures support this policy, ensuring accessibility for all RCC users, including students, faculty, staff, and the public.

Definitions:

- **Information and Technology:**
  Any hardware, software, digital and electronic applications, websites, documents, enterprise software, multimedia, audiovisual systems, communication devices, and any electronic or digital services that enable users to access, store, transmit, or manipulate information.
- **Equally Effective:**
  An alternative digital format that communicates the same information and provides a comparable experience in a timely manner. For interactive applications or service pages,

"equally effective" means the end result (e.g., registration) is achieved in a comparable time with similar effort.

Technical Standards:

- **Web Standards:**
  All web pages, websites, and web-based software published, hosted, or contracted by RCC (including remotely hosted sites and software) must meet the most recent standards and guidelines outlined in the Web Content Accessibility Guidelines (WCAG) from the World Wide Web Consortium (W3C). All RCC web pages must meet, at a minimum, WCAG 2.1 success criteria (levels A and AA), with limited exceptions. Where technically feasible, RCC webpages should link to the RCC Accessibility page, which includes a statement of commitment to web accessibility.
- **Software Standards:**
  All web-based software must meet WCAG 2.0 first- and second-level success criteria. Non-web-based software will follow the "Guidance on Applying WCAG to Non-Web Information and Communications Technologies" and must meet Section 508 Standards for Electronic and Information Technology (updated January 2018).
- **Hardware Standards:**
  Hardware should be operable by individuals with disabilities and compatible with assistive technologies. It must comply with Section 508 Standards for Electronic and Information Technology (updated January 2018) and the 2010 ADA Standards for Accessible Design, where applicable.
- **Application of Standards:**
  - **Applications and Core Content (Required to meet standards):**
    Institutional websites and all digital applications and services used to conduct business must meet WCAG 2.1 standards or have an equally effective access plan.
  - **Instructional Content (Required to meet standards):**
    Digital and electronic instructional materials, tools, and resources must meet accessibility standards or have an equally effective access plan.
  - **Non-business, Non-instructional (Recommended but not required):**
    Personal pages, archival materials, and student work should include an accessibility statement specifying how accommodation requests can be made.

Responsibilities:

- **Divisions, Departments, and Work Units:**
  Responsible for supporting RCC staff in obtaining training and technical support to ensure the accessibility of their digital content. They must also participate in efforts to document progress in increasing accessibility through program reviews and audits.

- **RCC Staff Responsible for ITAP:**
  The Access and Disability Resource Coordinator, IT staff, web team, and other designated personnel are responsible for reviewing accessibility standards, ensuring compliance, and providing training or technical support. Departments purchasing IT, educational software or hardware must consult with the Access and Disability Resource Coordinator.

Requests for Exceptions:
Any division, department, or individual seeking an exception to this policy must submit a written request to the Access and Disability Resource Office and a recommendation for an equally effective alternative. If approved, the Access and Disability Resource Office will work with the requesting party to develop a compliance timeline or alternative solution.

Reporting Access Issues:
Accessibility concerns can be reported to the Access and Disability Resource Office at (541) 956-7337 or via email -- accessoffice@roguecc.edu.

Related Policies, Procedures, and Information:
Rogue Community College

- RCC Online Learning Accessibility AP108b
- RCC Commitment to Equity, Diversity, and Inclusion
- RCC Nondiscrimination Policy
- RCC Human Resources

External
- Americans with Disabilities Act
- Web Content Accessibility Guidelines (WCAG 2.0)
- Section 508 of the Rehabilitation Act of 1973
- Section 504 of the Rehabilitation Act of 1973
- Accessibility of Web Content and Mobile Apps

TICKETING SYSTEM

Overview:

An IT ticketing system is a robust software platform that manages and tracks technical support requests. It creates an organized and efficient environment where users can submit support requests (tickets), and IT staff can handle, prioritize, and resolve these requests systematically. The system incorporates various features such as assignment, prioritization, escalation, communication, and reporting. The primary goal of an IT ticketing system is to streamline the support process, enhance response times, and provide improved visibility into the status of support requests.

Strategy:

1. The College's End User Support is available to assist all internal staff members.
2. The College maintains a ticketing system to track all issues and requests against a unique identifier. This system notifies requesters of their ticket information for reference.
3. The College assigns a Priority Level to each issue logged with the help desk. The Priority Levels are defined as follows:

Ticket Priority Level	Definition
Urgent	Critical college impact – problems that prevent the college's business from continuing. No workaround is possible. Examples: The data center is unavailable or classroom technology is offline.
High	Problems that do not currently halt the college, but their consequences could interrupt or stop business within 24 hours. Examples: Email is intermittently available.
Normal	Problems cause minor operational impact, or staff have lost functionality, but there is a workaround. For example, an error prevents rebooting a desktop computer.
Low	Issues with limited impact on production systems. Example: Need an application installed on a computer.

4. Each ticket priority level has specific response times, as described below:

Ticket Priority Level	Initial Response Time	Target Resolution Time
Urgent	~1 hour	As Soon As Possible

High	<4 hours	6 hours
Normal	< 1 Business Days	2 days
Low	< 2 Business Days	3-5 days
Scheduled	> 5 Working Days	By Arrangement

5. All issues are responded to within the timeframes specified above.
6. Typically, user requests sent via standard email to ithelpme@roguecc.edu are addressed during standard business hours. Urgent requests should be logged via telephone at 541.956.7042 to ensure prompt service.
7. The College provides escalation points for situations where the IT Department staff agrees that resolving an issue requires support from outside the project team.

Procedure to Process Tickets:

Stage 1: Ticket Triage and Assignment

- **Notification:**
  End User Support staff receive notifications of new tickets via email or directly within the ticket system dashboard.
- **Triage and Priority Assignment:**
  Following Rogue Community College's Service Level Agreements (SLAs), staff perform a triage to determine the ticket's priority. The appropriate priority is then assigned.
- **Technician Assignment:**
  The ticket is assigned to the appropriate IT technician(s) or IT Group based on the nature and priority of the issue.
- **Urgency Handling for 'Now' Priority:**
  If a ticket is triaged and found to require 'Now' priority, the staff ensures that the assigned technician is immediately aware of the urgency.

Stage 2: Initial Actions

- **Technician Assignment:**
  The technician begins work on the ticket, ensuring they are identified as the responsible technician. The ticket status should be updated to 'In Progress.' If the ticket is initially assigned to a group, the first technician to begin work will take ownership and assign themselves.
- **Ticket Assessment:**
  The technician reviews the ticket details to assess the nature and scope of the issue. Additional communication with the user may be necessary to gather further information or clarify the problem.

- **Adherence to Priority Levels:**
  The technician adheres to the priority level assigned per Rogue Community College's SLAs, guiding the time frame and resources allocated for resolving the ticket.

Stage 3: Resolution and Communication

- **User Communication:**
  Maintain clear and regular communication with the user throughout the ticket process. Responses should be detailed and informative, starting with a proper greeting and appropriate salutations. Additional context should be provided to reassure the user that their issue is being taken seriously.
- **Problem Resolution:**
  Utilize available resources and expertise to resolve the issue. If specialized attention is required, escalate the ticket to the appropriate group or a higher-level technician. Ensure that all steps taken before escalation are documented.

Stage 4: Ticket Closure

- **Ticket Status:**
  Upon resolution, mark the ticket as 'Resolved' if the issue was successfully addressed. If the issue was handled with a canned response, mark it as 'Closed.'

Documentation and Review

- **Documentation:**
  Document all steps, solutions, and relevant notes within the ticket system for future reference.
- **Review and Feedback:**
  Review closed tickets regularly to identify recurring issues and assess individual and team performance. Feedback from end-user surveys collected after ticket resolution can be valuable for continual service improvement. Complex or difficult tickets should be discussed in End-User Support meetings for collective training and feedback.

Understanding Ticket Statuses

- **On Hold and Scheduled:**
  These are system default statuses. 'Scheduled' is a copy of 'On Hold,' and both statuses pause any active timers related to the ticket.
- **Asana Project:**
  This status indicates that the ticket has been moved from the IT ticketing system to project management for more extensive handling and tracking.

- **Awaiting Response Closure Pending:**
  This status should be applied if an end user does not respond to a ticket within five days. After marking a ticket with this status, the system sends reminder emails to the end user for three days. If no response is received during that period, the ticket is automatically closed.

This procedure ensures that all IT issues are addressed systematically, promptly, and efficiently, providing high-quality support to users.

PROJECT MANAGEMENT SYSTEMS

Overview:

Rogue Community College (RCC) recognizes the critical role of project management systems in ensuring successful project execution. These systems facilitate the planning, execution, monitoring, and completion of projects while enhancing collaboration, transparency, and accountability. The following guidelines and processes are designed to standardize the use of project management systems at RCC, covering project creation, task assignment, progress tracking, communication, reporting, and system auditing. Thus, they promote consistency in project management and improve organizational efficiency.

Strategy:

1. **Objective:**
   The primary objective is to ensure the consistent and efficient use of project management systems across the college to achieve successful project outcomes. This manual aims to foster collaboration, streamline processes, promote transparency, and enhance accountability.
2. **Scope:**
   This manual applies to all IT staff members involved in project management activities within the college, including IT Department staff, project managers, team leads, and any other employees contributing to a project.
3. **System Use:**
   The college's project management systems will be used exclusively for business-related tasks and projects. Personal use or any use that deviates from the intended purpose is prohibited.
4. **Data Integrity:**
   All users must ensure the accuracy and completeness of the data input into the system, which is crucial to supporting accurate decision-making and reporting.

5. **Confidentiality:**
   Confidential and sensitive project information should only be shared with authorized individuals, and users must adhere to the college's data privacy and security guidelines.
6. **Training:**
   All users must receive appropriate training on using the project management system effectively.

Process:

1. **Project Creation:**
   When a new project is approved, the project manager (PM) or IT technician creates it in the project management system, including all necessary details including, but not limited to, as the project name, description, start date, end date, and team members.
2. **Task Assignment:**
   The PM creates tasks within the project, assigns them to team members, and sets deadlines. All assignments should be documented within the system.
3. **Monitoring Progress:**
   The PM should regularly monitor the status of tasks and overall project progress within the system. Any changes or updates should be promptly reflected in the system.
4. **Communication:**
   The project management system should serve as the primary mode of communication for all project-related discussions. This ensures that all team members have access to the same information and that important details are not lost in emails or separate conversations.
5. **Reporting:**
   The PM should regularly generate reports from the system to review progress, identify bottlenecks, and make informed decisions. These reports should be shared with stakeholders according to the reporting schedule.
6. **Project Completion:**
   Upon project completion, the PM should close the project in the system, ensuring all tasks are marked as completed, all documents are uploaded, and all lessons learned are documented.
7. **Auditing and Review:**
   The IT Department will periodically audit and review the use of the project management systems to ensure adherence to this manual and process and identify improvement opportunities.

ELECTRONIC COMMUNICATIONS

Overview:
Electronic communication is integral to various roles and activities at Rogue Community College (RCC) and includes the following mediums:

- **Email:**
  The official communication method at RCC for students and employees is used daily for conducting business. It is a fundamental tool for formal and informal communication, file sharing, and notifications. Despite some drawbacks, the benefits of email communication make it essential to use this medium effectively, efficiently, and as intended.
- **VoIP (Voice over Internet Protocol):**
  Enables voice calls over the internet, often integrating features such as voicemail, call forwarding, and teleconferencing.
- **Fax:**
  Used for transmitting scanned documents, particularly those requiring signatures or official seals.
- **Videoconferencing:**
  Facilitates virtual meetings and remote collaboration with video and audio capabilities.
- **Digital Signage:**
  For displaying dynamic or static information across various locations on campus.
- **Collaboration Platforms (e.g., Microsoft Teams):**
  Includes tools for real-time messaging, file sharing, team collaboration, and integration with other communication services. For example, Teams offers a unified platform for chat, calls, meetings, and collaboration, adaptable to various educational and administrative needs.
- **Instant Messaging and Social Media Platforms:**
  Facilitate rapid, informal communication and community engagement. These platforms range from direct messaging services for quick internal communications to broader social media networks that enable engagement with the larger college community, alumni, and external stakeholders. Examples include WhatsApp, Slack, and institution-specific Facebook or LinkedIn groups. While not primarily used for formal communication, these platforms play a significant role in fostering connectivity and a sense of community within and around the college.

Guidelines:
Regardless of the technology used, electronic communication at RCC serves the college's information-sharing needs with students, employees, vendors, state agencies, campus visitors,

and others. While each communication method has unique considerations that must be addressed individually, general rules help ensure that each method is used wisely and as intended.

RCC's electronic communication mechanisms should be used to disseminate information to all stakeholders. It is essential to understand that 'information sharing' at RCC involves conveying appropriate knowledge to support, not hinder, the College mission. This information should always be distributed under the following assumptions:

Electronic communication from an RCC resource:

- Is considered an official statement from the institution.
- Must never be used to create or distribute disruptive, offensive, derogatory comments or any information that could sabotage institutional progress or expose personally identifiable information.
- Must not be used for personal gain or excessive personal use.
- Must not be used to distribute malicious or harmful software or information.
- Is subject to public records requests and is discoverable.
- Is not private to the individual and can be reviewed by an appropriate manager when necessary.

MASS EMAIL

Overview:

This section outlines the guidelines and procedures for using mass email communication within Rogue Community College (RCC). Mass email is a powerful tool for distributing information to a large number of recipients simultaneously. The responsible use of this tool is essential to respect recipients' time and attention and maintain the integrity of RCC's communication systems.

Guidelines:

1. **Purpose and Scope:**
   Mass emails to faculty, staff, or students at RCC are intended to communicate official information that is urgent or related to emergencies, policy updates, administrative announcements, academic updates, or approved college-wide events. This section applies to all staff, faculty, students, and administrators who send or receive mass emails using RCC's email system.

2. **Authorization:**
   Only authorized RCC personnel may send mass emails. Authorization must be provided by the relevant vice president or their designee.
3. **Content Guidelines:**
   All mass emails must adhere to the following content guidelines:
   - Content must be relevant to the RCC community.
   - Content must align with RCC's mission, vision, and values.
   - Content must not contain any form of advertisement or promotion for personal gain.
   - Content must not include any offensive or inappropriate material.
4. **Opt-Out Provisions:**
   Mass emails sent to students' personal email addresses or the public must include an opt-out mechanism, allowing recipients to stop receiving such communications. These opt-out requests must be honored promptly. Mass emails sent to staff email accounts (@roguecc.edu) and student email accounts (@student.roguecc.edu) do not require an opt-out mechanism.
5. **Frequency:**
   Mass emails should be sent sparingly to avoid overwhelming recipients and maintain this communication tool's effectiveness.
6. **Privacy:**
   Mass emails must respect privacy. The BCC field should be used to protect recipients' email addresses unless it is essential for recipients to see who else received the message. Personal data should never be shared without explicit consent from the individuals involved.
7. **Technical Guidelines:**
   To ensure the functionality and security of RCC's email system, mass emails should avoid large attachments. Instead, provide links to files on a secure internal or cloud-based server. Do not use mass emails to distribute large data files or messages with high-resolution images or videos that could overload the server.
8. **Non-Compliance:**
   Non-compliance with these guidelines may result in disciplinary action, including employee termination or student expulsion. Severe violations may also result in legal action.

Conclusion:
These guidelines ensure that mass email is used effectively and responsibly within the RCC community as a critical communication tool. Adherence to these guidelines helps maintain the integrity of communication systems and respects the time and attention of all recipients. The IT

department will regularly review and update these guidelines to ensure their relevance and effectiveness.

PHISHING EMAIL

Overview:

This section outlines Rogue Community College's (RCC) practices for identifying, handling, and reporting phishing emails. Phishing is an online scam where malicious actors send fake emails that appear to be from reputable sources to steal sensitive information such as usernames, passwords, and credit card details.

Guidelines:

1. **Purpose and Scope:**
   This section aims to protect RCC's digital assets, including its network, systems, data, and the personal information of students, faculty, and staff. It applies to all users of the RCC email system, including students, faculty, volunteers, third-party vendors, Board Members, staff, and administrators.
2. **Identification:**
   Phishing emails often display telltale signs, such as:
   - Urgent or threatening language.
   - Requests for sensitive information.
   - Spelling and grammar mistakes.
   - Mismatched or suspicious-looking email addresses.
   - Links to unofficial or insecure websites.

All users of the RCC email system should familiarize themselves with these signs and remain vigilant in identifying potential phishing emails.

3. **Handling Suspected Phishing Emails:**
   If an email is suspected to be a phishing attempt:
   - Do not respond to the email.
   - Do not click on any links or download any attachments in the email.
   - Do not provide any personal information or sensitive data.
4. **Reporting:**
   - **Using the Report Button in Outlook or Outlook Online:**
     Select the suspicious email and click the "Report Phishing" or "Report to Sophos" button. This tool alerts the IT team directly and provides the necessary details without altering the email content.

- **Forwarding the Email:**
  Alternatively, forward the email to ThreatReport@roguecc.edu. Do not alter the subject line or the content of the email, as this information is valuable for the investigation. This method is helpful if accessing email from a client or platform where the report button is unavailable.

5. **Training and Education:**
   RCC will regularly provide students, faculty, and staff with training and educational resources on identifying and handling phishing emails. Participation in these training sessions is mandatory for all RCC employees.
6. **Monthly Phishing Awareness Campaign:**
   The IT Department at RCC will conduct a monthly phishing simulation campaign designed to mimic real phishing attempts and enhance cybersecurity awareness across the college.
   - **Campaign Details:**
     Each month, simulated phishing emails will be sent to staff and students. These emails are safe but resemble actual phishing attempts in appearance and content.
   - **Response to Being 'Caught':**
     If a simulated phishing email is interacted with (e.g., clicking a link or opening an attachment), the user will be directed to complete a brief, informative training session lasting no more than 10 minutes.
   - **Objective:**
     The primary goal of this campaign is education, not reprimand. Learning to recognize and appropriately respond to these simulated threats prepares users to identify actual phishing attempts in the future.
   - **Feedback and Improvement:**
     Participation and feedback from these campaigns are crucial. They help refine training materials and strategies to ensure the RCC community remains safe and informed about cybersecurity threats.

Conclusion:
Phishing is a serious threat to digital security and privacy. Mitigation can be achieved by following these guidelines, and the RCC community can protect its digital assets. The IT department will regularly review and update this section to ensure it remains effective against evolving cyber threats.

GUEST/VISITOR ACCESS AND TECHNOLOGY USE

Overview:
Rogue Community College (RCC) promotes openness and inclusivity by providing guests and visitors with access to our resources. However, this access must not compromise the integrity of our systems or the information they hold, nor should it introduce malicious software or intent into our internal network. All-access is governed by AP 3720 (Computer and Network User) and AP 3721 (Information Technology Acceptable Use).

Access Guidelines:
Guest and visitor access at RCC is categorized into two types:

1. **Standard Access:**
   Provides access to internet resources and online institutional resources through RCC Wi-Fi.
2. **Special Access:**
   Special access extends beyond standard access to include certain internal resources. It is granted only upon request by an authorized individual, such as a Vice President, the President, or a designated representative.

Special Access may include but not limited to:

- Wired networks (e.g., housing, guest)
- Single or multiple file access
- Access to systems like Blackboard, the ID Card System, etc.

Visitors must not be granted special access without explicit permission from the appropriate administrative personnel. This permission must be documented with a signature from one of the authorized individuals detailing the access granted.

For vendor access, please refer to this document's specific vendor access section.

These guidelines aim to balance openness with security at RCC. While welcoming guests and visitors, protecting our technological resources and the information they contain is also essential. The RCC IT Department regularly reviews and updates these guidelines to address potential threats and ensure alignment with industry standards.

Room Rental:
https://www.roguecc.edu/webforms/riskManagement/eventRequest.asp

REMOTE ACCESS

Overview:
Rogue Community College (RCC) recognizes that employees may need remote access to college resources to perform administrative duties effectively. To maintain the security and integrity of its network and data, RCC uses a Remote Desktop Services (RDS) solution. This section outlines the conditions for granting remote access and the procedures for obtaining and using such access under AP 7239 (Working Remotely).

Guidelines:

1. **Authorized Use:**
   Remote access to RCC's network is limited to active employees who require it to fulfill their professional responsibilities.
2. **Authentication:**
   RCC uses Okta, a multi-factor authentication (MFA) solution, to ensure that only authorized individuals gain remote access. Users must authenticate via Okta before accessing the RDS solution.
3. **Access Point:**
   Users can access the RDS solution at https://remote.roguecc.edu.
4. **Data Security:**
   All remote users must adhere to RCC's data protection and information security guidelines. Any violations may result in the suspension of remote access privileges and could lead to disciplinary action.
5. **Software and Hardware:**
   RCC does not maintain or support personal devices used to access the RDS solution. Users are responsible for ensuring their devices have updated antivirus software and are malware-free.

Procedure for Obtaining Remote Access:
Refer to AP 7239

VENDOR/CONSULTANT ACCESS

Overview:
The Vendor/Consultant Access guidelines outline the protocols vendors must follow when accessing Rogue Community College's (RCC) internal or external networks, workstations, or servers. These guidelines apply to all vendors, regardless of visitation frequency, the nature of

the work, or the entity's size, in accordance with AP 3720 (Computer and Network User) and AP 3721 (Information Technology Acceptable Use Policy).

Guidelines:
Vendors are required to notify their campus contact about any work requiring access to RCC resources, including but not limited to:

- Internal or external networks
- On-campus workstations or servers
- Network Infrastructure
- Other computing devices on campus

When access is needed, the RCC IT Department will create the necessary login credentials and establish access parameters to support the vendor's tasks. This access will initially be restrictive, limiting unnecessary or unwarranted access until the project's requirements dictate otherwise. Each access request will be evaluated individually to ensure appropriate access is granted.

Vendors are required to:

- Focus solely on their job responsibilities.
- Avoid breaching or bypassing the granted access.
- Refrain from altering security settings on existing network infrastructure or devices.
- Ensure that access credentials are not shared with unauthorized individuals.
- Protect RCC's information from loss or theft.
- Avoid disclosing any information obtained while working with RCC technology resources to third parties.
- Promptly notify the RCC IT Department if there is a suspicion of loss, theft, tampered access, or any other access violation.
- Refrain from using RCC's information for personal or financial gain.
- Refrain from misuse of access or technology resources prohibited for employees, students, or visitors under other guidelines.

Vendor Access Procedure:
If a vendor requires access to technology resources, the following steps will be taken:

1. Submit the Authorization of User Access Form to the RCC IT Department.
2. The IT Department will review the request and grant access based on need and existing policies.
3. The vendor's access will be configured in compliance with current policies.
4. The requesting employee will be notified via email once the appropriate access has been set up.

This section ensures RCC's technology resources are used responsibly and securely, protecting the institution's sensitive information and system integrity.

INFORMATION SENSITIVITY

Overview:
This section guides Rogue Community College (RCC) stakeholders on classifying, handling, and disclosing information based on its sensitivity level. These guidelines align with AP 3300 (Public Records), AP 5040 (Education Records, Directory Information and Privacy), AP 5045 (Student Records: Challenging Content and Access Log), AP 3710 (Securing of Copyright), and AP 3715 (Intellectual Property). They apply to all data formats used within RCC's operations.

Classification:
Information is categorized as either Public or Confidential. Public Information may be disclosed by authorized personnel, while Confidential Information, including third-party confidential data, is restricted and requires protection.

Handling Guidelines:
Sensitivity levels, ranging from minimal to More Sensitive, determine the protocols for accessing, distributing, storing, and disposing of information. Adherence to these guidelines ensures data integrity, availability, and confidentiality, which is in accordance with AP 3710 and AP 3715 principles.

Electronic Messaging Guidelines:
These guidelines ensure that proprietary, confidential, and sensitive information is securely exchanged. They promote responsible behavior in handling sensitive information under AP 3300.

Enforcement:
Following these guidelines upholds respect for intellectual property, protects networks and systems, and ensures responsible use of IT resources. This adherence aligns with AP 5040, AP 5045, and AP 3715, supporting RCC's commitment to institutional effectiveness and legal compliance.

PERSONALLY IDENTIFIABLE INFORMATION

Overview:
This section outlines RCC's definition of Personally Identifiable Information (PII) and sets guidelines for what PII, if any, may be shared with third-party entities. This manual aims to ensure the utmost respect for and protection of PII within the RCC community, which aligns with industry standards following BP 5040 (Education Records, Directory Information, and Privacy) and AP 5040 (Education Records, Directory Information and Privacy).

Guidelines:
Information should not be shared without a compelling reason, with exceptions made only for instances where state or federal government regulations require it, such as for annual reporting, compliance with state and federal regulations, compliance with grants and contracts, and public records requests. Information may also be shared during the course of institutional operations, vendor agreements, or upon the request of RCC's President or their appointed representative.

Personally Identifiable Information (PII) is data that should be safeguarded with the highest level of security. PII is defined as information about an individual that identifies, links, relates, is unique to, or describes them. This includes, but is not limited to, the following data:

- Name
- Social Security Number (SSN)
- Address(es)
- Phone Number(s)
- Email Address(es)
- Birth date
- Birth place
- Mother's maiden name
- Family names
- Other family data such as addresses, contact information, etc.
- Financial information such as bank account details, credit card details, account balances, etc.
- Other information that, alone or in combination, can be linked to a specific student or employee. Without personal knowledge of the relevant circumstances, a reasonable person in the campus community can identify the student or employee with reasonable certainty.
- Information requested by a person who the educational agency or institution believes knows the student's or employee's identity to whom the academic or other record directly relates.

PII should not be transmitted via email to external accounts, as external email communication is inherently insecure. For internal communications within RCC, where emails are encrypted, PII may be shared with a legitimate interest between staff members. Always err on the side of caution by transmitting only the minimum amount of data necessary to complete the task. On-campus storage of PII must comply with the guidelines outlined in this document. Any off-campus access to PII must be done through RCC Remote Access procedures or Secure websites (HTTPS) to ensure secure handling. For external communication, PII should be shared using secure, authorized methods, such as encrypted file transfer systems.

Sharing PII with third parties should only occur if necessary for RCC's legitimate educational interests or business operations, required by law, or if the student or employee has provided written consent.

The RCC IT Department is responsible for ensuring the secure storage, transmission, and destruction of PII in accordance with industry best practices. This includes using encryption for electronic data and secure locations for storing electronic documents.

All staff will receive training to ensure understanding and compliance with this manual.
This section will be reviewed annually to meet legal requirements, college policy, and current industry standards.

MULTIFACTOR AUTHENTICATION

Overview:
Rogue Community College (RCC) enhances system security by implementing Multifactor Authentication (MFA) on applications as deemed appropriate.

Guidelines:

1. Each system requiring a login will undergo a comprehensive analysis to determine if MFA integration is available and evaluate the feasibility of implementing this additional security layer.
2. MFA will be enabled whenever reasonable and practical.
3. MFA may include a combination of the following authentication methods, in addition to the primary username and password:
    - Phone Call
    - Text Message

- Authentication Application (e.g., Okta Verify for Staff, Microsoft MFA for Students)
- Google Authenticator

4. Each application secured by MFA will undergo an annual review to ensure the accuracy and relevance of secondary credentials.

Staff:
Staff members use Okta for multifactor authentication (MFA). This involves using the Okta Verify application to generate an authentication prompt. Staff authenticate by approving the prompt on their device or using a time-based one-time password (TOTP) generated by the Okta Verify app. This additional security layer helps protect access to network resources and facilitates secure password resets.

Students:
Currently, students do not use MFA to access RCC resources. However, starting in the winter term of 2026, students must also use Okta for MFA. Similar to the process for staff, students will use the Okta Verify application to generate an authentication prompt, approving the prompt on their device or using a TOTP generated by the app. This will provide enhanced security for accessing RCC systems.

Please note that, in line with best security practices, email cannot be used to deliver MFA tokens or other MFA-related items. This measure prevents unauthorized access if an email account is compromised.

Implementing MFA safeguards RCC's digital resources and protects individual user identities, helping maintain the integrity and confidentiality of RCC's digital ecosystem.

WIRELESS ACCESS

Overview:
Wireless connectivity is an essential resource for the Rogue Community College (RCC) community, providing faculty, staff, and students with reliable internet access. Any compatible data communication device is permitted to connect to the RCC wireless network for internet use. However, connecting to the RCC wireless network does not provide access to the internal networking infrastructure or internal information. Internal networks and information must be accessed through the remote RDS server.

This section outlines RCC's wireless network guidelines and provides additional details related to AP 3720 (Computer and Network Use) and AP 3721 (Information Technology – Acceptable Use).

Guidelines:

1. **Device Eligibility:**
   All wireless data communication devices (e.g., personal computers, smartphones, tablets) capable of transmitting packet data are eligible to connect to RCC's wireless network.
2. **Usage Scope:**
   The RCC wireless network is intended solely for external internet access. Access to RCC's internal network requires access through the remote RDS server.
3. **Security Measures:**
   Users must adhere to RCC's security protocols to ensure the safe and secure use of the wireless network.
4. **Compliance:**
   When using the wireless network, all users must comply with college policies and procedures, as outlined in AP 3720 and AP 3721.

Details:

1. The RCC wireless network is open, meaning no username or password is required for connection. While this offers easy access, users should be aware of the security risks associated with open networks and follow recommended practices for secure online behavior.
2. RCC's wireless and wired networks are separate entities that do not communicate or share information. This separation enhances security, preventing potential threats from spreading between them.
3. The IT Department manages wireless frequencies in the same way it manages the wired network. All college policies regarding computing apply to both wired and wireless networks.
4. The IT department provides and installs wireless access points, which allow devices to connect to the network. No other departments are permitted to set up access points without coordination with IT.
5. Other devices operating on the same radio frequency spectrum can cause interference with the wireless network. In such cases, IT will investigate and work with the individual to determine if the device can continue to be used without causing interference.

6. The IT Department reserves the right to disconnect any unauthorized access point discovered on the RCC network to ensure the integrity and security of the network infrastructure.

By following these guidelines, the integrity, security, and efficiency of RCC's wireless network can be maintained for the benefit of all users.

PERSONAL TECHNOLOGY

Overview:

This section outlines the scope and limitations of assistance the RCC IT Department provides regarding personal technology devices. While many individuals rely on their personal devices for various tasks, the RCC IT Department cannot offer comprehensive services for these devices for several key reasons:

- **Primary Responsibility:**
  The IT Department's main responsibility is ensuring the stability, security, and functionality of RCC's network and technology infrastructure, which requires significant resources and attention.
- **Device Variability:**
  The RCC community's wide range of personal devices presents challenges. Each device has unique specifications, software, and potential issues that require specialized knowledge and training to address effectively.
- **Liability and Warranty Concerns:**
  Working on personal devices may raise liability and warranty issues, leading to complications for the College and the device owner.
- **Service Disruption:**
  Providing extensive support for personal devices could interfere with essential services, such as network maintenance, software updates, and hardware troubleshooting for RCC-owned equipment.

Guidelines:

Given these factors, the following guidelines have been established:

- The RCC IT Department does not provide personal device repair, maintenance, or advanced troubleshooting services.
- The only service offered for personal devices is basic assistance connecting them to the RCC wireless network.

It is recommended that a professional technology service provider address advanced issues with personal technology devices.

Thank you for understanding and cooperating with these guidelines. This approach allows the IT Department to focus on its primary duty of maintaining and improving RCC's technological infrastructure.

DATA LOSS PREVENTION

Overview:
Data Loss Prevention (DLP) is a crucial component of Rogue Community College's (RCC) security strategy, designed to identify and prevent the inappropriate sharing, transfer, or use of sensitive data. This section outlines the methods and procedures in place to safeguard data across all platforms, ensuring compliance with laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and the Family Educational Rights and Privacy Act (FERPA).

Critical Components of DLP:

1. **Understanding Data:**
   A comprehensive understanding of the data landscape is essential. This involves identifying and classifying critical data across RCC's hybrid environment, including local and cloud storage. Special attention is given to data regulated by FERPA, such as student education records.
2. **Data Protection:**
   Protective measures are employed to secure data, including encryption, access restrictions, and visual markings. Encryption tools like BitLocker Drive Encryption are used on school-issued devices to protect against data theft or exposure from lost, stolen, or decommissioned computers. Access to FERPA-protected data is restricted to individuals with legitimate educational interests.
3. **Preventing Data Loss:**
   A culture of data security is promoted to help team members avoid accidentally sharing sensitive information, including FERPA-protected data. Regular training and awareness programs on data security and FERPA compliance are integral to this effort.
4. **Data Governance:**
   Best practices for data retention, deletion, and storage are followed to ensure compliance with laws and regulations, including FERPA. This involves maintaining accurate and secure student records and properly disposing of these records when they are no longer needed.

DIGITAL DATA RETENTION PROCEDURE

Overview:
The Information Technology (IT) Department at Rogue Community College (RCC) is committed to managing and retaining digital data in compliance with federal and state laws and institutional guidelines. This section outlines the data retention duration and the data disposal procedures.

Guidelines:

- All data managed by the IT Department, including those governed by FERPA, HIPAA, and GDPR, will be retained for the minimum period required by applicable federal or state law. No data will be knowingly destroyed before the legally mandated retention period. If these laws change, the IT Department will update its practices to comply with the new retention periods.
- Data will not be removed, discarded, or destroyed in any manner that could jeopardize legal compliance, data integrity, or RCC's institutional needs. Retention timeframes will be maintained as long as RCC requires access to the data, provided this does not conflict with legal requirements for data storage or destruction. Data will not be destroyed before the timeframe or retained beyond the legally specified period.
- To safeguard critical data from corruption or loss, the IT Department uses backup equipment, off-site storage, regular backup schedules, and data restoration practices. In cases of data loss, corruption, or when recovery is necessary, priority will be given to restoring institutional data.
- This procedure does not shorten the retention periods mandated by state or federal law but may extend the retention period based on RCC's needs. Any extension will only be implemented if it does not compromise the data storage system’s integrity, storage capacity, or performance.

By following this procedure, the IT Department at RCC ensures a strong, compliant digital data management framework that protects individual privacy, secures sensitive information, and supports the college's institutional needs.

RCC BACKUP

Overview:
The Information Technology (IT) Department at Rogue Community College (RCC) manages systems to store and retain essential digital data for each department securely. This central storage area, known as the group drive, enables robust backup capabilities to ensure data is recoverable in the event of a disaster or other data loss incidents.

This section outlines the regular backup schedules for group drive storage devices and applies to all stored data. It does not cover data stored locally on individual, departmental, or computer lab devices, mobile devices, or other portable storage mediums, and the IT Department cannot guarantee backup for these types of devices or storage mediums.

Guidelines:

- All RCC departments and employees are strongly encouraged to store sensitive, important, and confidential data on their respective group drives. The IT Department is not responsible for data stored elsewhere.
- Regular nightly backups are scheduled for group drive storage devices. Additionally, quarterly restore tests are conducted on key systems to ensure the reliability of the backup system and the recoverability of data.
- If a file, folder, or collection of data is found to be missing, corrupt, or otherwise damaged, immediate notification to the IT Department is required. Delays in reporting decrease the likelihood of successful recovery.
- The IT Department’s Disaster Recovery Plan (DRP) and Backup Priority List (BPL) provide guidelines for large-scale recovery needs affecting multiple departments or institutions.
- The IT department's backup hardware includes two storage devices: a primary device and a secondary, off-site device. The primary device serves as the central storage and backup hub, holding all data and backups. The secondary device replicates all data from the primary device, creating a secure off-site copy for added protection.

This section describes the backup process based on the current configuration, considering the hardware in use. Regular nightly backups and quarterly restore tests ensure that RCC's data remains secure and accessible, contributing to the robustness of the college's data management infrastructure.

STORING DATA ON ONEDRIVE AND TEAMS

Overview:
Rogue Community College (RCC) is migrating personal H: drive data to OneDrive and

departmental drive data to Teams to streamline data storage and collaboration. A key aspect of this transition is the careful handling of Personally Identifiable Information (PII) to ensure data privacy and compliance.

Procedure:

1. **Review of Existing Data:**
    - Departments and individuals must thoroughly review their current data stored on H: drives and departmental drives.
    - The focus of this review is to identify and segregate any data containing PII.
2. **Handling PII Data:**
    - Data containing PII must remain on network drives located on campus.
    - Access to PII data should be restricted and subjected to strict security measures.
    - Staff accessing PII data must follow high-level security protocols to prevent unauthorized access or breaches.
3. **Migration of Non-PII Data:**
    - Data not containing PII should be migrated to OneDrive (for personal data) and Teams (for departmental data).
    - This migration will facilitate better access, collaboration, and backup of RCC's digital assets.
4. **Training and Guidelines:**
    - The IT Department will provide training sessions and guidelines for staff on identifying PII, securely handling sensitive data, and migrating data to OneDrive and Teams.
    - Best practices for organizing and managing data within OneDrive and Teams will be included in the training.
5. **Security and Compliance Checks:**
    - Regular security audits and compliance checks will be conducted to ensure that data storage practices comply with privacy laws and RCC’s data protection guidelines.
    - Emphasis will be placed on ensuring that no PII data is inadvertently stored on OneDrive or Teams.
6. **Ongoing Support:**
    - The IT Department will offer ongoing support and assistance throughout the migration process.
    - A dedicated support channel will be established to address any queries or issues related to the migration.
7. **Documentation and Record Keeping:**

- Detailed records of the migration process, including data reviewed, data migrated, and security checks, will be maintained.
- This documentation will serve as a reference for compliance audits and future data management initiatives.

HARDWARE LOSS PREVENTION

Overview:
Rogue Community College recognizes the critical role digital assets play in the educational environment. This includes hardware such as computers, laptops, tablets, and other portable devices vital to daily operations. However, these assets are also vulnerable to loss or theft, which could result in data breaches or costly replacements.

Guidelines:

1. **Asset Management:**
   The college will maintain a detailed inventory of all hardware assets. Each asset will be recorded with specific information, including make, model, serial number, configuration details, assigned user, and location. Regular audits will be conducted to ensure accuracy and accountability.
2. **Secure Usage and Storage:**
   Hardware assets must be used and stored securely at all times. Portable devices should be securely locked when not in use or left unattended. Staff and students are prohibited from leaving college-owned hardware in public spaces, unlocked vehicles, or other unsecured environments.
3. **Personal Responsibility:**
   Each staff member and student is personally responsible for the hardware assets assigned to them. This includes maintaining the device's physical security, using the hardware following college policies, and promptly reporting any issues or concerns.
4. **Reporting Loss or Theft:**
   Any hardware loss or theft must be reported immediately to the IT department. The IT department will document the incident, take steps to secure or disable the device remotely if possible, and report the incident to RCC's Risk Management Department.
5. **Return of Assets:**
   All hardware assets must be returned when a staff member or student leaves the college. Similarly, when an asset is no longer needed or due for replacement, it must be returned promptly. Unreturned hardware may be considered stolen property, leading to appropriate consequences.

6. **Compliance and Auditing:**
   The IT department will conduct regular compliance audits to ensure adherence to these guidelines. Any violations will be addressed, and the responsible individual may face disciplinary action. These audits also serve as a feedback mechanism for improving policy effectiveness.

RCC INTERNET RESOURCES

Overview:
This section outlines guidelines for the responsible, professional, and efficient use of RCC's internet communication resources. These guidelines apply to all RCC employees, students, and affiliates using the college's internet service.

Guidelines:

1. **Acceptable Use:**
   RCC's internet resources are to be used for legitimate educational purposes, research, or the conduct of college business. Personal business, personal gain, or activities unrelated to the college's mission are prohibited. Unacceptable use includes but is not limited to, promoting personal ventures, illegal activities, or participating in online gambling. Refer to AP 3721 (Information Technology - Acceptable Use) for complete details.
2. **Professional Conduct:**
   All users are expected to use the Internet responsibly and productively. Communication should remain professional, courteous, and respectful at all times. Language that could be interpreted as discriminatory, sexually explicit, threatening, or otherwise offensive must be avoided. Users are representatives of RCC and should conduct themselves accordingly.
3. **Respect for Privacy:**
   Users must respect the privacy of others and refrain from sharing personal information about individuals without explicit permission. This includes private communications, photographs, or confidential information. RCC values the dignity and privacy of all members of its community and expects these values to be upheld.
4. **Secure Communications:**
   Sensitive or confidential RCC-related information must only be shared through secure, approved communication methods. Unsecured channels should not be used to protect the integrity of RCC's information systems and the confidentiality of its data.

5. **Use of College Resources:**
   Using RCC's internet and communication resources for illegal activities, personal gain, or commercial purposes unrelated to the college's mission is strictly prohibited. These resources are shared assets and should be used with that in mind.
6. **Intellectual Property:**
   Users are required to respect copyright laws and fair use principles. This includes not sharing copyrighted material without authorization and properly crediting original authors in research and assignments.
7. **Monitoring and Compliance:**
   RCC reserves the right to monitor internet usage and communications on its network to ensure compliance with these guidelines. Users should be aware that their activities are not entirely private and may be reviewed if there is a suspected violation of college policy.
8. **Responsibility:**
   Each user is responsible for their actions on the internet and for adhering to these guidelines. Ignorance of the guidelines is not an excuse for noncompliance. Users are encouraged to contact the RCC IT Department for guidance if clarification is needed.
9. **Disclaimer:**
   While RCC strives to provide secure, reliable, and uninterrupted internet access, internet communications' security, reliability, or privacy cannot be guaranteed. Users should be mindful of this when using RCC's internet resources and take appropriate steps to protect their privacy and data.

   By accessing RCC's network and using the Internet service provided, users agree to follow this Internet Communication Policy. Non-compliance may result in a review by the appropriate college authorities. Depending on the severity of the violation, consequences may include temporary or permanent loss of access privileges and referral to disciplinary channels within the college. For questions or clarification about this policy, don't hesitate to contact the RCC IT Department.

OFFICE/COMPUTER ACCESS BY IT DEPARTMENT STAFF

Overview:
IT staff members at Rogue Community College may need to access campus computers and offices to resolve technical issues. These guidelines are designed to protect the privacy and security of college staff and students while allowing IT personnel to perform their duties effectively.

Guidelines:

1. **Authorized Access:**
   Only properly trained and authorized IT staff members may access campus computers and offices to address technical issues. Authorization must be granted by the Chief Information Officer (CIO) or a designated authority.
2. **Special Access for VP and President Offices:**
   For the offices of Vice Presidents and the President, explicit permission must be obtained from the respective office holder before any IT staff member can access the area or computers. This permission must be documented and retained for future reference.
3. **Access Procedure:**
   When accessing a computer or office, IT staff members should first attempt to notify the owner or occupant. If the owner or occupant is not present, a note must be left indicating the access's date, time, and purpose.
4. **Privacy and Confidentiality:**
   IT staff members are expected to respect individuals' privacy and confidentiality when accessing computers and offices. They should not view, copy, modify, or share files or information unless necessary to resolve the technical issue.
5. **Notification for Major Upgrades or Projects:**
   The IT department will notify supervisors in advance when conducting large upgrade projects or other significant IT tasks in their area. This ensures smooth coordination and minimal disruption to daily operations.
6. **Documentation:**
   IT staff members must document all instances of access to campus computers and offices. The documentation should include the date, time, location, purpose of access, and any actions taken.

USER ACCOUNTS

Overview:

User accounts and groups are critical to the IT infrastructure at Rogue Community College, allowing individuals to access and utilize the College's IT resources. This section provides a framework for creating, managing, and using user accounts and groups to maintain a secure and efficient IT environment.

Guidelines:

1. **User Account Creation:**
   Only authorized IT staff may create user accounts. Each account must be assigned to a single individual who will be responsible for all actions taken using that account.
2. **User Groups:**
   User groups should be created based on roles, departments, or specific projects. These groups help manage permissions and access rights, simplifying processes and improving security.
3. **Account Responsibility:**
   Account holders are responsible for maintaining the security of their accounts. This includes setting strong passwords, not sharing credentials, and promptly reporting any suspicious activity.
4. **Access Rights and Permissions:**
   Access to IT resources must follow the "least privilege" principle, granting individuals only the access necessary for their roles. Regular audits should be conducted to ensure appropriate access rights and permissions.
5. **Account Termination:**
   When an individual leaves the College or no longer requires access to certain IT resources, their account or specific access rights must be promptly deactivated.

USER ACCOUNT CREATION

Overview:
This section outlines the procedures for creating user accounts, assigning system access rights, terminating user accounts, and locking or disabling accounts. These procedures ensure that all RCC systems and data are accessed securely and used appropriately.

Scope:
These guidelines apply to all RCC employees, contractors, consultants, temporary employees, and other workers, including third-party personnel.

Guidelines:

User Account Creation:

1. The IT Department creates user accounts based on information provided by the Human Resources (HR) Department during the hiring process.
2. Each new user account is assigned a unique user ID and a temporary password, which the user must change upon first login.

3. Access rights and permissions are granted based on the user's job responsibilities, ensuring no user has more access than necessary for their role.

User Account Naming Convention:

1. RCC follows a standardized naming convention for all user accounts to maintain consistency and ease of identification. The convention is based on the user's legal or preferred name, as provided by the HR Department.
2. The standard format is the first initial of the user's first name, followed by their full last name (e.g., John Smith's user ID would be "JSmith").
3. In the event of a duplicate (two users with the same first initial and last name), the user's middle initial is added between the first initial and last name (e.g., "JASmith" for John Adam Smith).
4. If a user's name changes (due to marriage, preferred name, or legal change), the HR Department will notify the IT Department to update the user ID.
5. The IT Department reserves the right to modify the naming convention to ensure unique user IDs. Any changes will be communicated to all users.

User Account Assignment:

1. Access rights are assigned based on the principle of least privilege, meaning users receive only the minimum access needed to perform their job functions.
2. The IT department regularly reviews and adjusts access rights. Significant changes in job responsibilities should be reported to the IT Department to ensure appropriate access rights.

User Account Sharing and Password Management:

1. Sharing RCC user accounts and passwords is strictly prohibited. Each user account is unique and must only be used by the designated individual.
2. Users are responsible for keeping their passwords confidential. Passwords should not be written down, sent via unencrypted communication, or shared with anyone.
3. If a user suspects their account has been compromised, they should immediately notify the IT Department and change their password.

Administrator and Elevated Accounts:

1. Administrator or elevated accounts provide higher access rights than typical user accounts. These accounts are typically used for tasks like software installation or system configuration.
2. These accounts are strictly controlled and must be requested in writing, with a detailed explanation of the need for elevated access.

3. All requests for administrator or elevated accounts must be approved by the Chief Information Officer (CIO), who will instruct the IT Department to create the account if approved.
4. Elevated accounts are subject to the same password and account sharing policies as regular user accounts and should only be used for tasks requiring elevated privileges.
5. These accounts are regularly audited to ensure appropriate use. Misuse may result in disciplinary action, including termination of employment or contract.
6. The IT Department and CIO will periodically review elevated accounts to ensure they remain necessary. Accounts no longer needed or found to violate RCC policies will be disabled or deleted.

Account Locking and Disabling:

1. RCC has implemented procedures to lock or disable accounts to enhance system security and prevent unauthorized access.
2. Accounts may be locked or disabled under the following circumstances:
   a. After a set number of unsuccessful login attempts to prevent brute-force attacks.
   b. When suspicious activity is detected, such as attempts to access unauthorized resources.
   c. When an individual's employment or association with RCC is terminated.
   d. When an individual is on a leave of absence.
3. The IT Department manages account locks and disables accounts as needed. Accounts are unlocked only after verifying the user's identity and addressing the issue that caused the lock.
4. Users with locked or disabled accounts should immediately contact the IT Department for assistance.
5. Attempts to bypass account locks or access a disabled account may result in disciplinary action, including termination of employment or contract.

Review and Termination of User Accounts:

1. The IT Department periodically reviews all active user accounts. Accounts no longer needed or found to violate RCC policies may be disabled or deleted.
2. The HR Department provides the IT Department with a list of employees who have left RCC. The IT Department will disable those accounts within 24 hours of receiving this information.
3. If a user's employment or association with RCC ends outside of regular HR reporting (e.g., leave of absence), the account may be temporarily disabled within 24 hours of notification.

4. During a leave of absence, accounts may be temporarily disabled instead of fully deactivated, following the same 24-hour timeframe.

GUEST ACCOUNT PROCEDURES

Overview:
The Guest Account Procedures govern using guest accounts on RCC's IT systems. These accounts are to be used only as a last resort for student and staff sign-ins, with precautions to ensure appropriate and secure use.

Procedure:

1. **Purpose of Guest Accounts:**
    - Guest accounts provide temporary access to RCC's IT systems in exceptional circumstances.
    - These accounts serve as a contingency option when students or staff are unable to use their credentials.
2. **Preference for Personal Credentials:**
    - All efforts should be made to assist students and staff in signing in with their credentials.
    - Support for credential recovery or account troubleshooting must be provided before resorting to a guest account.
3. **Use of Guest Accounts:**
    - Guest accounts should only be used when all attempts to resolve sign-in issues with personal credentials have failed.
    - These accounts should be used sparingly to ensure the security and integrity of RCC's IT systems.
4. **Security and Confidentiality:**
    - The username and password for any guest account must not be displayed publicly or shared with students, staff, or community members.
    - RCC staff should enter guest account credentials directly, maintaining confidentiality.
5. **Monitoring and Auditing:**
    - Guest account usage will be monitored and audited to ensure compliance with this procedure.
    - Logs of guest account usage will be maintained, including details of who accessed the account, the duration, and the purpose.
6. **Account Limitations and Restrictions:**

- Guest accounts will have limited access rights, providing only the necessary resources for the user's needs.
- These accounts will not have access to sensitive or personal data and will be restricted from making system changes or adjusting settings.

7. **Account Expiry and Deactivation:**
   - Guest accounts are temporary and will have a predetermined expiry date.
   - Accounts will be deactivated immediately after their intended use or expiry date.
8. **Procedure Compliance:**
   - All RCC staff must adhere to this procedure. Any misuse or unauthorized use of guest accounts will result in the removal of the account.
   - Regular training and awareness programs will ensure staff understand the procedure and the importance of guest account security.

GROUP ASSIGNMENT AND MANAGEMENT

Overview:
This section outlines the procedures for creating, managing, and terminating user groups within RCC IT systems. Effective group management ensures that access to resources and data is appropriately and securely managed.

Scope:
These procedures apply to all RCC employees, contractors, consultants, temporary employees, and other workers within the IT Department, including personnel affiliated with third parties.

Guidelines:
Group Creation and Assignment:

- The IT Department is responsible for creating user groups. A new group must be requested in writing, justifying its need.
- Users are assigned to groups based on their job responsibilities. Each user may belong to one or more groups as required.
- Access rights are assigned to groups rather than individual users. This simplifies access management and ensures that all users within a group have the same access level.
- The IT Department maintains an updated list of all active groups, their members, and their access rights. This list is reviewed and updated periodically.

Group Management:

- The IT Department manages security user groups, including adding and removing users, modifying access rights, and creating or deleting groups.

- Changes to group membership or access rights must be requested through the IT Department in writing, including a justification for the change.
- The IT Department periodically reviews group membership and access rights. Adjustments to group membership may be necessary if a user's job responsibilities change.
- When users leave RCC or move to a different department, they are removed from all IT Department groups. Supervisors are responsible for notifying the IT Department of these changes.

Group Termination:

- Groups are terminated when they are no longer needed. The IT Department makes this decision after consulting with relevant stakeholders.
- Upon termination, all users are removed from the group, and the group's access rights are revoked.
- Group termination is performed in a way that minimizes disruption to users and systems, with users being notified in advance.
- After a group is terminated, the IT Systems Department conducts a review to ensure that all access rights have been revoked and no residual data remains.

PASSWORD GUIDELINES

Overview:

This password policy establishes a standard for creating, protecting, and regularly updating passwords within RCC's IT Department to ensure secure system access.

Guidelines:

General Password Construction Requirements:

All RCC users, including contractors and vendors with access to RCC systems, are responsible for selecting and securing their passwords according to the following guidelines:

- Must be at least 12 characters in length.
- Must include at least one uppercase letter (A-Z).
- Must include at least one lowercase letter (a-z).
- Must include at least one number (0-9).
- Must include at least one special character (e.g., !, @, #, $, %).
- Must not contain any part of the username.
- Must not include the user’s first or last name.
- Must not be identical to any of the last four passwords used.

Password Change and Expiration Requirements:

- All user-level passwords (staff and faculty) must be changed every 365 days.
- Elevated account-level passwords must be changed every 90 days.
- Users will receive notifications when their passwords are due to expire and must follow the prompts to update their passwords.
- If a password violates the standards at any time, it must be changed immediately, and the associated account will be locked until the password is updated to meet the guidelines.

Password Protection Standards:

- Passwords must not be shared with anyone, including administrative assistants, managers, colleagues, family members, or friends.
- Passwords must not be inserted into emails, notes, or other forms of electronic communication.
- Passwords must not be displayed or revealed in any public space.
- Passwords must not be written down and left unsecured.
- Passwords must not be stored in a computer or mobile device file without encryption.

Password Managers and Web Browser Storage:

- RCC's IT Department approves 1Password as the exclusive password manager for securely storing and managing passwords. All users are encouraged to use 1Password for this purpose. For more information, contact the IT Department.
- Storing passwords in web browsers is not recommended due to security risks. Always deny 'save password' prompts when entering credentials in web browsers.

USER ENVIRONMENT

Overview:

This section outlines guidelines for properly using and managing user environments within the RCC IT Department. It covers desktop images, third-party applications, USB external drives, and other user environment elements, intending to protect the integrity of RCC's IT systems and data.

Guidelines:

- **Desktop Environment:**
  The desktop environment must remain clean and organized. The RCC IT Department sets desktop images, and personal customization, including changing the desktop image, is not permitted without IT Department approval.

- **Third-Party Applications:**
  Installing third-party applications requires prior approval from the RCC IT Department to avoid software conflicts, security risks, or potential viruses. Approved applications must be appropriately licensed, compatible with existing systems, and necessary for business operations. All college procurement policies must be followed when purchasing new software.
- **USB/External Drives:**
  The RCC IT Department must approve the use of USB or other external storage devices. These devices present security risks as they can be lost, stolen, or used to introduce malicious software into the network. Data stored on these devices must be encrypted and backed up to protect the information in case of loss or theft.
- **End of Shift Protocol:**
  Users must log off their systems but leave their computers powered on at the end of their shift. This allows the IT Department to perform system maintenance, updates, and other necessary tasks during off-hours.
- **System Maintenance and Updates:**
  Users are not permitted to disable or interfere with system updates or maintenance tasks initiated by the IT Department. These updates are essential for system security and performance. Any issues or concerns should be reported to the IT Department.
- **Physical Security:**
  Users must ensure the physical security of their computers by locking them when not in use and preventing unauthorized access.
- **Training and Awareness:**
  Users are strongly encouraged to participate in regular training and awareness sessions organized by the IT Department. These sessions will cover the latest IT security practices, potential threats, and policy updates.

COMPUTER PURCHASING

Overview:
This section outlines the procedures and guidelines for procuring computer hardware and software at Rogue Community College (RCC). The goal is to ensure that all hardware and software acquisitions are efficient, cost-effective, and aligned with RCC's IT standards.

Goals:

1. Standardize the procuring of computer hardware and software processes across all college departments.

2. Ensure all hardware and software purchases meet technical and functional requirements.
3. Promote the efficient and cost-effective acquisition of hardware and software.
4. Support responsible IT resource use and safeguard sensitive data throughout the college.

Hardware and Software Standards:

1. The IT Department enforces standardization of software and hardware platforms to ensure compatibility and reduce support costs.
2. Within RCC's IT ecosystem, only hardware and software that meet technical requirements and are approved by the IT Department are allowed.
3. All hardware and software purchases must comply with licensing requirements and relevant laws.

Procurement of Non-Desktop/Laptop Hardware:

1. **Requirement Identification:**
   Staff must define their hardware and software needs based on departmental requirements and budget.
2. **Quote Request:**
   Staff must request quotes from End User Support before making purchase decisions. This ensures IT is informed and can provide feedback on technical compatibility, cost, and vendor reputation.
3. **Security, Accessibility, and Privacy Assessment:**
   All purchases must comply with RCC's security, accessibility, and privacy policies to prevent vulnerabilities, ensure accessibility, and uphold privacy standards.
4. **Vendor Selection:**
   After evaluating quotes, the IT Department selects vendors based on competitive pricing, quality, and delivery times in compliance with college policy.
5. **Budget Request Process:**
   - **Initial Request:**
     Departments initiate the process by requesting a quote or needs assessment from IT, ensuring compatibility, security, and cost estimation for the ActionPak.
   - **ActionPak Creation:**
     Departments use the provided information to create an ActionPak item in their budget.
   - **CIO Review:**
     The CIO reviews each ActionPak with a technology component to ensure strategic alignment and feasibility.

- **Approval and Fund Transfer:**
  Approved ActionPaks result in fund transfers to the IT Department for procurement.

6. **Purchase Order:**
   Once a vendor is selected, the IT Department issues a purchase order, adhering to RCC's procurement policies.
7. **Delivery and Installation:**
   The IT Department handles the installation and configuration of ordered hardware and software.
8. **Acceptance Testing:**
   The IT Department conducts acceptance testing post-installation to verify that the hardware and software meet technical requirements and perform as expected.

Computer Replacement and Purchase Restrictions:

1. **Five-Year Replacement Cycle:**
   The IT department automates and manages this process, which involves replacing staff and faculty computers on a five-year rotation.
2. **Laptop Procurement and Replacement:**
   - **Request Submission:**
     Individuals needing a laptop must submit the 'Laptop Needs Form' at https://ithelpme.roguecc.edu.
   - **Evaluation:**
     The IT Department reviews requests and may consult with the requester to determine specific needs.
   - **Purchase Authorization:**
     Laptop purchases are approved based on an evaluation of the request, ensuring alignment with RCC's use case criteria.
   - **One Computer Per User Standard:**
     RCC adheres to a 'One Computer Per User' standard to manage costs and resources. Exceptions require CIO approval.
   - **Replacement:**
     Laptop replacements follow the same procedure, with justifications provided through the 'Laptop Needs Form' and IT approval.
   - **Maintenance and Repairs:**
     The IT Department handles laptop maintenance and repairs. Users must report issues through designated IT support channels.

Asset Management:

1. The IT Department maintains an inventory of all hardware and software assets, including manufacturer, model, serial number, and purchase date.
2. The asset management database is regularly updated to ensure accuracy.
3. The IT Department manages the disposal of hardware or software that is no longer in use or has reached end-of-life in compliance with relevant regulations.

Conclusion:
This policy guides the procuring of computer hardware and software at RCC. It ensures transparency, accountability, and cost-effective acquisition while aligning purchases with the college's IT standards. The IT Department will periodically review and update this policy to ensure continued relevance and effectiveness.

COMPUTER REPLACEMENT CYCLE

Overview:
Maintaining modern and functional technology is essential for productivity and efficiency at Rogue Community College. The IT Department manages a proactive computer replacement cycle to ensure that hardware used by staff, faculty, and students remains up-to-date. This section outlines the computer replacement process.

Procedures:

- **Five-Year Replacement Cycle:**
  The IT Department follows a five-year rolling replacement cycle for all staff, faculty, and classroom computers. Based on hardware inventory data, this schedule ensures that technology stays current, reliable, and secure.
- **Automatic Replacement Schedule:**
  Staff and faculty do not need to request computer replacements. The IT department automatically schedules replacements for computers nearing the end of their five-year cycle.
- **Notification of Replacement:**
  - The IT Department will notify staff or faculty members five days before the scheduled replacement to arrange a suitable time, ensuring minimal disruption to daily work or teaching activities.
  - This advance notice allows ample time to prepare to transition to the new computer.
- **Replacement Process:**
  The replacement process includes setting up the new computer with all approved software applications. Personal files will not be transferred; all critical files should be

stored on network drives or approved cloud storage solutions. IT will provide training on any new features or systems during the new computer's delivery.

- **Decommissioning of Old Computers:**
  Old computers will be decommissioned and disposed of following e-waste recycling guidelines.
- **Early Replacement in Case of Issues:**
  If a computer experiences significant problems before the end of its five-year cycle, staff or faculty should contact IT immediately. The IT Department will assess the situation and repair or replace the computer as necessary.
- **Adaptability of the Replacement Cycle:**
  The IT Department reserves the right to adjust the replacement cycle based on technological advancements, funding availability, or changing user needs.
- **Ownership and Usage:**
  All computers remain the property of Rogue Community College and must be used responsibly following college policies.

NEEDS ASSESSMENT FOR NEW TECHNOLOGY OR PROJECTS

Overview:
The Information Technology (IT) Department at Rogue Community College supports all academic and administrative functions. This procedure outlines the approach for responding to new technology needs or projects initiated by various departments. The primary objective is to ensure that technology requests are handled systematically, efficiently, and effectively, resulting in solutions that address the department's needs and align with the college's strategic goals.

1. Initial Meeting:
Engage with the requesting department to understand their specific needs and expected outcomes. This involves gathering detailed information about their requirements.
2. On-Site Evaluation:
Conduct an on-site evaluation to assess the department's current operations and determine how the new technology will integrate with their workflow.
3. Feasibility Study:
Evaluate the project's viability by considering the following aspects:

- **Technical Feasibility:**
  Assess whether the project is technically feasible with existing or new resources. For example, does the requested software require higher computing power or specific hardware that is currently unavailable?

- **Economic Feasibility:**
  Perform a cost-benefit analysis to determine if the benefits, such as increased productivity or efficiency, justify the project's cost.
- **Operational Feasibility:**
  Evaluate how the project will impact daily operations. Will it require significant changes to the department's workflow, and is there a risk of disruption during the transition?

4. Solution Design:

Develop a solution based on the department's needs and the feasibility study's findings. This may include researching software vendors, comparing features and prices, or considering custom development if off-the-shelf solutions are unsuitable. In complex projects, this phase may involve creating prototypes or mockups.

5. Budget Request Process:

- **Initial Request:**
  Departments request a quote or need assessment from IT to ensure compatibility, security, and cost estimation for the ActionPak.
- **ActionPak Creation:**
  Departments create an ActionPak item in their budget based on the information provided by IT.
- **CIO Review:**
  The CIO reviews each ActionPak with a technology component to ensure strategic objectives and feasibility alignment.
- **Approval and Fund Transfer:**
  Approved ActionPaks lead to fund transfers to the IT Department for procurement.

6. Presentation of Proposed Solution:

Present the proposed solution to the department in a clear and concise manner. The presentation should include:

- A detailed description of the solution
- How it addresses the department's needs
- Expected benefits and potential drawbacks
- Implementation timeline
- Project budget
  Use visual aids like diagrams or slides to help communicate the points effectively.

7. Feedback and Revision:

Collect feedback from the department and revise the proposed solution based on their input. Multiple rounds of feedback and revision may be necessary to ensure the solution fully meets the department's requirements.

8. Implementation:
Implement the approved solution according to the agreed timeline. Maintain regular communication with the department and address any issues during the process.
9. Post-Implementation Review:
Conduct a review after implementation to ensure the technology meets the department's needs and expectations. This includes gathering user feedback, observing how the technology is utilized, and measuring its impact on departmental operations. Based on the feedback, make adjustments as necessary.

This procedure ensures that the IT Department effectively responds to new technology needs or projects, leading to successful implementations that support Rogue Community College's academic and administrative success.

STANDARD HARDWARE SPECIFICATIONS

For All Staff/Faculty:
Each staff and faculty office at Rogue Community College will be equipped with the following standard hardware configuration:

- Windows Desktop Computer
- Two 22” monitors
- Keyboard
- Mouse
- Headset
- Webcam

Laptop Provision:
Laptops are considered specialized equipment due to their higher cost and specific functionality. While they are not part of the standard hardware package for all staff, they may be provided under certain circumstances:

1. **Needs Assessment:**
   Staff or faculty members who believe their work requires hardware beyond the standard configuration must complete a detailed needs assessment. This evaluation determines if a laptop is the appropriate solution based on individual needs. A comprehensive rubric is used to evaluate the necessity of a laptop objectively. The needs assessment form is available at https://ithelpme.roguecc.edu.
2. **Rubric-Based Evaluation:**
   The rubric is a vital tool in the laptop request process. It evaluates the need for a laptop

based on various factors such as work location, data sensitivity, and software requirements. Although the specific scoring system is internal, it ensures that laptop allocation is aligned with institutional needs and resource management policies.

3. **Appeals Process:**
   Staff members may appeal the decision if a laptop request is not approved based on the rubric assessment. Appeals should be directed to the Director of IT, who will review the case alongside the needs assessment and rubric to ensure all factors have been considered fairly.
4. **Exceptions:**
   - **Departmental Requirements:**
     Due to the nature of their work, the Marketing Department often requires Apple Computers. Requests from this department will be honored without a separate needs assessment.
   - **Position-Based Privileges:**
     Staff at the level of Assistant Director or higher are allowed to request a laptop without undergoing the standard needs assessment, recognizing the mobile and varied nature of their roles.

CLASSROOM TECHNOLOGY ACQUISITION

Overview:
Technology plays a crucial role in education at Rogue Community College. The IT Department ensures that all classroom technology, including hardware and software, is up-to-date and functional, aligning acquisitions with educational goals to maintain a seamless learning environment.

Procedure:

- **Formal Request for Additional Technology:**
  All new classroom technology needs must be formally requested through the IT Department.
- **Justification for Technology Requests:**
  Faculty or administrative staff requesting new technology must provide a detailed justification outlining the proposed use, its impact on teaching and learning, and the benefit to students.
- **Needs Assessment and ActionPak Budgeting Process:**
  The IT Department conducts a comprehensive Needs Assessment for each request, evaluating factors such as educational value, compatibility, ease of use, lifecycle, and total cost. An ActionPak is created for budgeting purposes.

- **Time Frame for Requests:**
    - **Advance Notice Requirement:**
      Requests must be submitted at least 90 days before the expected implementation date to allow time for proper evaluation, procurement, and installation.
    - **Resource Management Consideration:**
      This timeframe is crucial to avoid disruptions in classroom availability and scheduling.
- **Prohibition of Unauthorized Installations:**
    - **Mandatory Approval:**
      No hardware or software should be purchased or installed in classrooms without prior approval from the IT Department.
    - **Risk Mitigation:**
      Unauthorized installations can result in compatibility issues, security risks, or unnecessary costs and may lead to the equipment being disallowed or unsupported.
- **Installation and Maintenance by IT Department:**
  The IT Department installs and maintains all approved classroom technology to ensure proper setup and optimal functionality.
- **Responsible Usage and Maintenance:**
  Proper care and responsible classroom technology usage are essential to maintaining its effectiveness and supporting an optimal learning environment.

HARDENING OF STAFF/STUDENT HARDWARE

Overview:
The protection and integrity of Rogue Community College (RCC) technology resources are critical to operations, privacy, and data security. This section outlines the guidelines for "hardening" hardware, a process aimed at reducing system vulnerabilities and safeguarding against potential threats. Hardening includes configuring system settings, updating and patching systems, and installing protective software.

Procedure:

- **Scope of Hardware Hardening:**
  All hardware used by RCC staff, faculty, and students—including desktops, laptops, tablets, and mobile devices—must be hardened according to IT Department standards.
- **Responsibility of the IT Department:**
    - The IT Department is responsible for hardening all hardware before deployment.

    - This includes the standard setup and configuration for staff and faculty hardware.
- **Hardening Procedures:**
  The hardening process, following industry best practices, includes:
    - Regular updates with the latest patches from vendors.
    - Installation and maintenance of security software, such as antivirus and antimalware.
    - Configuration of user access controls to limit access and ensure appropriate user privileges.
    - Disabling or removing non-essential services, applications, and network protocols.
    - Secure configurations for all hardware and software.
- **User Compliance:**
    - Staff, faculty, and students are prohibited from altering, disabling, or circumventing any security configurations established by the IT Department.
    - Exceptions to these guidelines require IT Department approval and will be considered case-by-case, particularly for academic or administrative needs.
- **Reporting and Vigilance:**
    - Users must adhere to these security measures and promptly report any suspected vulnerabilities or security issues to the IT Department at threatreport@roguecc.edu.
    - Regular security reviews and updates will be conducted to adapt to evolving threats.

PHYSICAL SECURITY OF STAFF/FACULTY EQUIPMENT

Overview:
Ensuring the physical security of technology equipment at Rogue Community College (RCC) is critical to the institution's information security strategy. This document establishes guidelines for safeguarding the physical integrity of staff and faculty equipment, whether in offices, classrooms, or used as mobile devices, to prevent unauthorized access, theft, or damage.

Procedure:

- **Responsibility for Equipment Security:**
  Staff and faculty are responsible for the physical security of all technology equipment assigned to them, including computers, laptops, tablets, mobile devices, and other work-related hardware.
- **Security in Offices and Classrooms:**

- Equipment in offices and classrooms should be secured when not in use. Desktop computers must be locked or signed out to allow for IT maintenance during off-hours.
- Portable equipment must be stored in secure locations when not in use.
- In shared spaces, collaboration is essential to ensure adherence to security measures.

- **Security of College-Owned Mobile Devices:**
  - College-owned mobile devices must not be left unattended in public areas.
  - When traveling or working off-campus, these devices should be kept with the individual or secured in a safe location to prevent loss, theft, or unauthorized access.
- **Handling and Care of Portable Equipment:**
  - All portable equipment must be handled carefully to avoid damage.
  - Protective cases are recommended for laptops and mobile devices, especially during travel.
- **Reporting Loss, Theft, or Damage:**
  - Any loss, theft, or physical damage to technology equipment must be reported immediately to the IT Department.
  - The IT Department will take action to remotely lock or wipe lost or stolen devices to protect sensitive data.
- **Additional Physical Security Controls:**
  - The IT Department may implement further physical security measures as necessary, such as cable locks for desktops and secure storage solutions for high-value or sensitive equipment.
- **Encryption of Hard Drives:**
  - **Mandatory Hard Drive Encryption:**
    All hard drives in RCC staff and faculty equipment, including desktops, laptops, and mobile devices, must be encrypted using EFS (Encrypting File System) or similar encryption software.
  - **Data-at-Rest Security:**
    This encryption ensures that data stored on these devices (data-at-rest) is protected, adding an extra layer of security.
  - **Implementation and Compliance:**
    The IT Department will oversee the implementation and maintenance of encryption, ensuring all devices comply with this requirement.
  - **Encryption Management:**
    Regular checks and updates will be conducted to maintain the effectiveness of

encryption protocols, adapting to new security challenges and technological advancements.

These measures are designed to prevent unauthorized access, theft, or damage to RCC's technology resources while maintaining the continuity and integrity of IT operations. Following these guidelines will help protect both hardware and its valuable data.

STAFF/FACULTY EQUIPMENT CHECKOUT

Overview:
Rogue Community College (RCC) recognizes that faculty and staff may need access to technology equipment for work-related activities outside of campus, including working from home. This section outlines the equipment checkout process, ensuring responsible use, timely resource return, and alignment with RCC's AP 7239 (Working Remotely policy).

Procedure:

- **Request for Technology Equipment:**
  Faculty and staff may request technology equipment from the IT Department for work-related use, including laptops, tablets, projectors, mobile devices, and other equipment for remote work.
- **Submission of Request:**
  Requests must be submitted formally to the IT Department, specifying the equipment needed, its purpose, and the expected checkout duration. If approved, the IT Department will review the requests and schedule a pickup.
- **Responsible Use and Care:**
  All checked-out equipment must be used responsibly and in compliance with RCC's IT policies, including adherence to AP 3720 (Computer and Network Use) for personal and college-issued equipment.
- **Alignment with Remote Work Policy (AP 7239):**
  - The checkout process follows RCC's Remote Work Policy, which requires discussion and approval for remote work and equipment checkout.
  - A Remote Work Agreement must be in place, detailing duties, performance expectations, work schedule, and other relevant terms.
- **Training on Equipment Setup and Takedown:**
  - **On Campus:**
    The IT Department will provide training for equipment setup and takedown and will handle these tasks for on-campus events and activities.

- **Off-Campus:**
  For off-campus events such as conferences or remote work, the requesting staff member is responsible for setting up and taking down the equipment.

- **Routine Maintenance and Equipment Return:**
  The IT Department may request that equipment be returned for maintenance. Equipment should be returned by the agreed-upon date, or an extension must be communicated beforehand.
- **Inspection and Accountability:**
  Upon return, the equipment will be inspected for damage or loss, with potential accountability for repair or replacement costs.
- **Work-from-Home Equipment:**
  The same policies apply to equipment used for work at home. Any issues or damage must be reported promptly.
- **Safety and Security in Remote Work:**
  Employees are expected to maintain a safe and secure remote work environment and adhere to RCC's safety standards and workers' compensation laws.

DESKTOP/CLASSROOM MAINTENANCE AND UPDATE

Overview:
Regular maintenance and updates of technology equipment are essential for ensuring the efficiency, security, and stability of Rogue Community College's (RCC) IT environment. This document outlines the responsibilities and procedures for maintaining and updating desktop computers and classroom technology.

Procedure:

- **Responsibility of IT Department:**
  The RCC IT Department is responsible for the regular maintenance and updates of desktop and classroom technology, which includes:
  - Routine system maintenance tasks.
  - Installing the latest operating systems, application software, and security updates.
- **Scheduling of Maintenance and Updates:**
  - Maintenance and updates are typically scheduled during off-hours to minimize disruption.
  - Users should not attempt system maintenance or updates themselves and are encouraged to report any issues to the IT Department.
- **User Cooperation in Maintenance:**

    - Equipment must remain powered on during scheduled maintenance periods.
    - Users are advised to lock or sign out of systems rather than shut them down to facilitate off-hours maintenance.
- **Notification of Scheduled Maintenance:**
    - For urgent fixes or security patches that require intervention during regular working hours, the IT Department will provide advance notice when possible.
- **Adherence to Best Practices and Emergency Updates:**
    - The IT Department follows a regular maintenance and update schedule in line with industry best practices.
    - In response to critical advisories from technology vendors or cybersecurity entities, emergency or out-of-cycle updates may be necessary. These updates will be communicated promptly, with efforts made to minimize disruption.
- **Communication and Training:**
    - For major updates or changes, the IT Department will provide relevant information and training to users, ensuring they are familiar with new features or system changes.

SOFTWARE MANAGEMENT AND STANDARDIZATION

Overview:
Software standardization is essential for maintaining consistency, reducing complexity, and improving productivity within Rogue Community College's (RCC) IT environment. This document outlines the approach to managing software to ensure a uniform working environment across all computers.

Objective:
RCC aims to create a unified, efficient, and secure software environment for staff, ensuring compliance with software licensing and adherence to best software management and standardization practices.

Procedure:

- **IT Department's Role in Software Management:**
  The RCC IT Department is responsible for procuring, installing, and managing all software on RCC computers, including operating systems, productivity tools, web browsers, and security software.
- **Standard Software Configuration:**
    - RCC maintains a base software configuration for all staff computers, ensuring a consistent working environment.

    - The standard setup typically includes the latest stable versions of essential software.
- **Approval Process for Additional Software:**
    - The IT Department must approve additional software installations required for specific job functions.
    - Requests are evaluated for compatibility, licensing, support, and security considerations.
- **Prohibition of Unauthorized Software Installation:**
    - Staff are not permitted to install software without approval from the IT Department.
    - Unauthorized installations can introduce compatibility issues, security vulnerabilities, and licensing violations.
- **Software Updates and Issue Reporting:**
    - The IT Department manages software updates in line with the desktop/classroom maintenance and update procedures.
    - Staff should report software issues to the IT Department for timely resolution.
- **Software Lifecycle and Strategic Alignment:**
    - Regular software reviews are conducted to ensure alignment with RCC's operational needs and strategic goals.
    - Software may be added, updated, or removed based on usage patterns, evolving needs, and its strategic fit.

STAFF/FACULTY SOFTWARE PROCUREMENT

Overview:
Procuring software at Rogue Community College (RCC) follows a structured process to ensure a secure, compliant, and standardized IT environment. This section governs the purchase of new software and Software-as-a-Service (SaaS) solutions for staff and faculty, ensuring alignment with legal, privacy, and usage considerations.

Procedure:

- **IT Department's Role in Software Procurement:**
  The RCC IT Department is responsible for procuring and installing all software on staff and faculty computers, including traditional software and SaaS subscriptions. The IT Department must approve all requests for new software or SaaS.
- **Integration with Needs Assessment Process:**
    - Requests for new software or SaaS solutions must clearly explain the need, intended use, and expected benefits.

    - The IT Department will conduct a needs assessment, evaluating requests based on compatibility with current systems, functionality, support availability, security implications, and cost-effectiveness.
- **Review of Legal and Compliance Documents:**
    - Staff and faculty must submit relevant documents, such as Privacy Policies, Terms of Service, or End User License Agreements (EULA), for review.
    - The IT Department will ensure compliance with RCC policies and regulations, including FERPA.
- **Licensing and Subscription Management:**
  The IT Department will manage all software licenses and subscriptions, ensuring ongoing compliance and proper software and SaaS solutions licensing.
- **Installation and Setup Protocols:**
  The IT Department is responsible for installing software and setting up SaaS solutions to ensure proper integration with RCC's IT systems. Staff and faculty are prohibited from installing software or setting up SaaS solutions without IT Department approval and assistance.
- **Reporting Concerns:**
  Any concerns or issues with the procurement process should be reported to the IT Department for resolution.

CLASSROOM SOFTWARE AND SAAS PROCUREMENT

Overview:
At Rogue Community College (RCC), maintaining an effective, consistent, and stable learning environment is essential. This section outlines the procedures for procuring software and Software-as-a-Service (SaaS) solutions for classroom use, emphasizing careful planning and coordination to minimize disruptions.

Procedure:

- **IT Department's Responsibility:**
  The RCC IT Department is responsible for procuring, installing, and managing all classroom software and SaaS solutions. The IT Department must approve all requests for new software or SaaS.
- **Integration with Needs Assessment and ActionPak Budgeting:**
    - Faculty requesting new software or SaaS for classroom use must submit a needs assessment, including an ActionPak item in their budget. This should detail the software's or service's educational value, intended use, and anticipated impact.

    - The ActionPak must include a cost-benefit analysis and ensure alignment with RCC's educational goals and budgetary constraints.
- **Compliance Review of Software or SaaS:**
  Required documents, such as the Privacy Policy, Terms of Service/EULA, and data handling practices, must be submitted for review to ensure compliance with RCC policies and regulations, including FERPA.
- **Evaluation Criteria for Software or SaaS:**
  The IT Department will evaluate the software or SaaS-based on compatibility with existing technology, educational value, support availability, security risks, and cost-effectiveness.
- **Communication and Timing of Requests:**
    - **Advance Notice for Requests:**
      Faculty must respond promptly to software change request emails and submit new software requests at least 90 days in advance, preferably before the term begins. This advance notice is essential to avoid implementation delays and minimize classroom disruptions.
    - **Requests After Term Start:**
      If a software request is made after the term has started, it must be carefully planned to avoid interfering with other classes in the same room. The IT Department will collaborate with the requesting faculty to facilitate the installation but may require patience as coordination with multiple stakeholders is needed once the term is underway.
      The IT Department will make every effort to accommodate these requests, ensuring minimal impact on ongoing classes and the overall learning environment.
    - **Software Changes During Term Breaks:**
      Software changes should preferably be made during term breaks or other suitable times to maintain classroom stability.
- **Installation and Setup Management:**
  The IT Department will manage the installation and setup to ensure proper integration and minimize classroom disruption.
- **Addressing Questions and Issues:**
  Faculty should direct any questions or concerns regarding classroom software or SaaS procurement to the IT Department.

SOFTWARE SUPPORT GUIDANCE

Overview:
This section defines the scope of responsibilities of the IT Department at Rogue Community College (RCC) regarding network servers and department-specific software packages. It clarifies the IT Department's limits in specialized software and outlines the protocol for departments seeking support and training for their unique software applications.

Procedure:

1. **IT Department Responsibilities:**
    - The IT Department is responsible for maintaining network servers and ensuring departmental software packages are current, properly installed, and functioning efficiently on the network.
    - This includes routine software updates and patches and ensures compatibility with RCC's overall IT infrastructure.
2. **Departmental Software Expertise:**
    - While the IT Department ensures the operational readiness of software, it does not provide expertise on the specific functionalities or usage of each department's specialized software.
    - Departments are responsible for acquiring the necessary expertise in using and managing their specialized software.
3. **Vendor Support and Contact:**
    - Departments are advised to directly contact software vendors for support on issues related to the software itself, including technical difficulties, software-specific errors, or functionality questions beyond the general maintenance provided by the IT Department.
4. **Educational and Training Responsibilities:**
    - Departments are responsible for obtaining how-to guidance and training on their specific software applications.
    - Departments should work with software vendors or use vendor-provided resources to train staff and understand the software.
5. **Communication and Coordination:**
    - Departments should notify the IT Department about significant software issues that may impact the network or other systems.
    - The IT Department will assist in communicating with vendors if network or system-wide issues are identified.
6. **Documentation of Vendor Contacts:**
    - Departments are encouraged to document interactions with software vendors, including support tickets, training sessions, and major software changes or updates.

- This documentation helps track software issues and resolutions and is a valuable reference for future needs.

7. **Compliance with IT Policies:**
   - All software maintained by the IT Department or individual departments must comply with RCC's IT policies and standards.
   - This ensures that all software used at RCC meets security, privacy, and compatibility requirements.

SERVER/NETWORK EQUIPMENT PROCUREMENT

Overview:
Rogue Community College (RCC) is committed to maintaining a robust and efficient IT infrastructure. A strategic five-year plan guides the procurement of server and network equipment to ensure alignment with college objectives, promote consistent performance, and optimize cost-effectiveness.

Procedure:

- **IT Department's Responsibility:**
  The RCC IT Department is responsible for overseeing the procurement of all server and network equipment. This includes adhering to the five-year plan and addressing urgent needs to maintain performance and security.
- **Annual Planning and Five-Year Plan Alignment:**
  - The IT Department conducts an annual assessment of the five-year purchasing plan to ensure it aligns with technological advancements, operational needs, and strategic goals.
  - This review process allows adjustments to the procurement strategy based on emerging technologies and changing requirements.
- **Regular Purchasing Process:**
  - The five-year plan specifies the types of equipment, projected lifespans, and replacement schedules.
  - Equipment not included in the plan must receive IT Department approval, accompanied by a detailed justification.
- **Urgent Purchasing Protocol:**
  - The IT Department may authorize off-schedule procurement in the event of unexpected equipment failure or when urgent upgrades are necessary for performance or security.
  - Justifications for these urgent purchases must be documented, clearly outlining the necessity and urgency.

- **Adherence to Standards and Best Practices:**
    - All equipment procured must meet industry standards for performance, security, and compatibility.
    - The IT Department evaluates proposed equipment based on these criteria to ensure compliance with best practices.
- **Management of Equipment Setup and Integration:**
  The IT Department manages the setup, installation, and integration of all procured equipment, ensuring proper functionality and compatibility with RCC's IT infrastructure.
- **Addressing Procurement Questions or Issues:**
  Any inquiries or concerns regarding server/network equipment procurement should be directed to the Director of IT for appropriate resolution.

SERVER/NETWORK EQUIPMENT DEPLOYMENT

Overview:
Efficient and thorough deployment of new server and network equipment is crucial for optimizing the performance and security of Rogue Community College's (RCC) IT infrastructure. This manual outlines the steps to ensure swift implementation and rigorous testing of new equipment to maintain a high standard of performance and security.

Objective:
The goal is to ensure that new server and network equipment is deployed efficiently and securely, with minimal disruption to RCC’s operations. This process supports RCC's educational and operational objectives while maintaining a state-of-the-art IT infrastructure.

Procedure:

- **Responsibility of the IT Department:**
  The RCC IT Department is responsible for deploying all new server and network equipment, including setup, integration, testing, and maintenance.
- **Prompt Deployment:**
    - New equipment will be set up and integrated into RCC's IT infrastructure within ten business days of receipt.
    - This quick deployment reduces downtime and ensures the new equipment is operational as soon as possible.
- **Comprehensive Testing:**
    - Rigorous testing, including performance assessments, compatibility checks, and security evaluations, is conducted prior to regular operation.
    - Equipment is only deployed after passing all necessary tests.

- **Collaborative Deployment Approach:**
    - For deployments affecting multiple departments, coordination with relevant personnel ensures minimal operational disruptions.
    - Advance notice is provided regarding any planned downtimes.
- **Detailed Documentation:**
    - All deployment steps, test results, issues, and resolutions are thoroughly documented for future reference and maintenance.
- **Training and Support:**
    - Training is provided to staff and faculty for any new workflows or procedures associated with the deployed equipment.
    - Ongoing support is offered post-deployment to address any additional needs or adjustments.
- **Feedback and Issue Resolution:**
    - The IT Department remains open to feedback after deployment and promptly addresses any performance or compatibility issues.

PHYSICAL SECURITY OF SERVER AND NETWORK ROOMS

Overview:
The security of server and network rooms, including Main Distribution Frame (MDF) and Intermediate Distribution Frame (IDF) rooms, is critical for protecting Rogue Community College's (RCC) IT infrastructure from unauthorized access, theft, or damage. This section outlines the measures in place to secure these vital areas.

Objective:
The aim is to ensure a high level of physical security for RCC's server and network rooms, safeguarding them against unauthorized access and potential threats while maintaining a secure and resilient IT infrastructure.

Procedure:

- **Collaboration with Risk Management:**
  The RCC IT Department collaborates with the Risk Management Department to uphold the physical security of all servers and network rooms. This includes managing access controls, surveillance, and conducting regular security audits.
- **Restricted Access:**
    - Access is limited strictly to authorized personnel.
    - All entries and exits are logged, with regular reviews for any anomalies.

- **Physical Access Controls:**
    - Robust access control systems, such as card or biometric scanners, are implemented to secure entry to these areas.
    - These systems are maintained and tested regularly to ensure reliability.
- **Annual Access Review:**
    - The list of personnel with access is reviewed annually to reflect current authorizations.
    - Adjustments are made based on changes in staff roles or responsibilities.
- **Monitoring Systems:**
    - Security cameras are strategically placed to monitor access points.
    - Any unusual activity captured by the cameras is investigated immediately.
- **Regular Security Audits:**
    - Jointly conducted by the IT and Risk Management teams, these audits assess potential vulnerabilities and ensure compliance with College policies.
    - Audits are scheduled to identify any security gaps or breaches.
- **Ongoing Security Training:**
    - IT staff with access to these rooms receive regular training on physical security protocols.
    - Training covers identifying security threats and the appropriate incident response procedures.
- **Emergency Response Plan:**
    - An emergency response plan is in place for handling security incidents related to these rooms.
    - The plan is regularly reviewed and updated to address new threats or changes in infrastructure.

REQUEST AND ORDERING OF IT EQUIPMENT

Overview:
This section outlines the guidelines for requesting and ordering IT equipment at Rogue Community College (RCC). It applies to routine procurements within the ongoing five-year plan and urgent or emergency orders outside the plan.

Objective:
This section ensures that IT equipment procurement is structured, justified, and aligned with RCC's goals while remaining compliant with institutional procurement policies.

Procedure:

- **Ordering within the Five-Year Plan:**
    - The Director of IT is authorized to approve orders for IT equipment that are part of the established five-year plan.
    - Orders must align with planned inventory needs and budgetary considerations.
- **Urgent or Emergency Orders:**
    - The CIO must approve any urgent or emergency IT equipment requirements outside the five-year plan.
    - These situations may include unexpected equipment failures, critical upgrades, or needs arising from changes in college operations.
- **Request Procedure for IT Personnel:**
    - IT personnel must submit equipment requests through the designated IT request system.
    - Requests should include the type and quantity of equipment, rationale for the request, and any other relevant information.
- **Evaluation of IT Requests:**
    - Each request is evaluated for its alignment with RCC's strategic goals, budgetary limitations, and overall IT infrastructure plan.
    - This ensures that all procurement decisions are strategic, necessary, and justifiable.
- **Compliance with Procurement Policies:**
    - All IT equipment procurement must follow RCC's established procurement policies and procedures.
    - This includes obtaining necessary quotes or conducting a Request for Proposal (RFP) process where required, ensuring fairness, transparency, and fiscal responsibility.

BACKUP FOR ON-PREMISES AND CLOUD-BASED DATA

Overview:

Rogue Community College (RCC) emphasizes the critical importance of data integrity and availability in academic and operational settings. This procedure outlines the unified backup process for RCC data, covering both on-premise and cloud-based storage solutions, to ensure resilience against disasters, hardware failures, or cybersecurity incidents.

Procedure:

1. **Scope:**
   This section applies to all data owned, used, or managed by RCC, regardless of its storage location (on-premise or cloud). It includes various data types such as

documents, emails, databases, multimedia content, and applications on physical and virtual servers.

2. **On-Premise Data Backups:**
   Regular backups of on-premise data are stored at secure off-site locations to protect against physical damage or disasters. RCC follows the 3-2-1 backup strategy: three copies of the data, two on different local mediums, and one stored offsite, ensuring robust data protection.
3. **Cloud Data Backups:**
   RCC adheres to the same stringent backup standards for data stored in the cloud using the 3-2-1 rule. Despite cloud services offering their own data replication across data centers, RCC independently manages its backups to ensure data availability in case of vendor-specific issues.
4. **Data Classification and Backup Schedules:**
   Data is classified based on its importance to RCC operations. Critical data is backed up more frequently, while less critical data follows a less frequent schedule, optimizing resource use while ensuring availability.
5. **Backup Verification and Practice Restores:**
   Backup integrity and restoration processes are regularly tested. Practice restores are conducted bi-annually to confirm the effectiveness of data recovery and ensure that backup data remains accessible and functional.
6. **Security of Backup Data:**
   Backup data is encrypted both at rest and in transit to ensure security. Physical security measures protect backup storage media from unauthorized access and data corruption.
7. **Retention of Backup Data:**
   Backup data retention periods are determined based on regulatory requirements, the importance of the data, and available storage capacity. After the retention period expires, data is securely destroyed or archived as needed.
8. **Disaster Recovery:**
   This backup policy is closely aligned with RCC's Disaster Recovery Policy, which outlines the procedures for data recovery and the resumption of operations after a data loss event.

SERVER HARDENING GUIDELINES

Overview:

The Server Hardening Guidelines establish minimum security configurations for all servers at Rogue Community College (RCC), both physical and virtual. These guidelines aim to prevent unauthorized access, data breaches, and other security incidents by addressing vulnerabilities

at the server level. They align with industry best practices from the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

Procedure:

1. **Scope:**
   These guidelines apply to all servers owned, operated, or maintained by RCC, whether physical or virtual, including those on-premise, hosted externally, or managed by third parties for the college.
2. **Physical Security:**
   - All physical servers must be stored in secure, access-controlled environments.
   - Access is restricted to authorized personnel, and all access attempts must be logged and monitored.
   - These measures comply with NIST Physical Security Guidelines.
3. **Software Security:**
   - Software, including operating systems, must be hardened according to CIS and NIST best practices.
   - Unnecessary software and services must be removed or disabled, and secure configurations must be applied.
   - Servers must follow CIS Benchmarks or equivalent security guidelines.
4. **Local Administrator Accounts:**
   - The default administrator account should be disabled.
   - A new local administrator account must be created following RCC's password management policies.
   - The principle of least privilege applies, in line with NIST SP 800-53, AC-2.
5. **Regular Updates and Patch Management:**
   - Regular updates and patches are mandatory for all server software.
   - A patch management strategy must be in place, following CIS Control 3, with scheduled updates and emergency procedures as needed.
6. **Security Monitoring and Logging:**
   - Continuous monitoring for security threats is required.
   - Security logs must be regularly generated and reviewed.
   - Any suspicious activities must be reported immediately.
7. **Backups and Disaster Recovery:**
   - Backup and disaster recovery procedures must follow RCC's established policies.
8. **Additional Security Measures:**
   - **Anti-Malware Software:**
     Approved anti-malware software must be installed on all servers.

- **OS Firewall:**
  The operating system's firewall must be enabled and properly configured.
- **Remote Management with Okta:**
  Okta Multi-Factor Authentication (MFA) must be used to secure remote server management.
- **Integration with RCC's SIEM and Network Monitoring:**
  All servers must be integrated with RCC's Security Information and Event Management (SIEM) and network monitoring solutions to enhance oversight and threat detection.

SERVER AUDITING AND MONITORING

Overview:
This section outlines the auditing and monitoring procedures for all Rogue Community College (RCC) servers and IT equipment. It highlights the use of Security Information and Event Management (SIEM) solutions to monitor network activity, detect potential security breaches, and provide real-time analysis of security alerts.

Procedure:

1. **Scope:**
   These guidelines apply to all servers (physical or virtual) and IT equipment owned, operated, or managed by RCC, regardless of location (on-premise, off-site, or in the cloud).
2. **Server and IT Equipment Monitoring:**
   Continuous monitoring of servers and IT equipment is required to track availability, performance, and any unauthorized or suspicious activities. Monitoring should cover network traffic, resource usage, and system events, with alerts triggered by unusual activity for immediate investigation by designated personnel.
3. **Security Information and Event Management (SIEM):**
   SIEM solutions must be deployed throughout RCC's IT infrastructure. SIEM agents should be installed on all servers and IT equipment to enable continuous network monitoring for potential security breaches. These tools collect and analyze log and event data in real-time, correlating information across systems to detect possible security incidents. The IT team must investigate all alerts generated by the SIEM system promptly.
4. **Audit Logging:**
   Audit logs must be enabled and maintained on all servers and IT equipment. These logs

should record events such as user login/logout activities, changes to user privileges, and system configuration updates to detect unauthorized activities or policy violations.

5. **Retention and Protection of Audit Logs:**
   Audit logs should be securely stored for a period specified by regulatory requirements and RCC's operational needs. They must be protected against unauthorized access, alteration, and deletion and encrypted both at rest and in transit.
6. **Regular Audit Reviews:**
   Audit logs must be regularly reviewed to identify anomalies or access violations. All findings should be documented, and any identified issues must be addressed without delay.
7. **Incident Response:**
   In the event of a security incident, the IT team will follow RCC's Incident Response Plan. Data from SIEM systems and audit logs will play a critical role in investigating and resolving the incident.

IT CHANGE MANAGEMENT

Overview:
The IT Change Management guidelines are established to manage changes within the IT environment in a controlled, systematic, and risk-averse manner. The goal is to minimize the negative impact of changes on services, ensure a high level of service quality, and maintain the integrity of ongoing IT operations.

Procedure:

1. **Scope:**
   These guidelines apply to all IT assets and services managed by Rogue Community College, including systems, applications, network equipment, servers, software, and hardware.
2. **Roles and Responsibilities:**
   The following roles manage and implement changes:
   - **Change Initiator:**
     Identifies and proposes the need for a change.
   - **Change Manager:**
     Oversees the change management process and ensures compliance.
   - **Assistant Director of IT/Director of IT:**
     Reviews, approves, or rejects proposed changes.

3. **Change Classification:**
   Changes are categorized as standard, normal, or emergency, requiring different authorization levels and procedures.
4. **Change Request Procedure:**
   All changes must be formally requested, documented, and recorded using a Change Request form. The request should include a detailed description of the change, the justification, potential impact, rollback plan, and other relevant details.
5. **Change Approval:**
   The Assistant Director of IT or the Director of IT must review and approve all change requests, assessing their potential impact and associated risks before approving.
6. **Implementation:**
   Approved changes must be implemented by trained personnel. Changes should be scheduled to minimize disruption to College operations.
7. **Testing and Validation:**
   After implementation, each change must be thoroughly tested and validated to ensure it achieves the intended results without compromising system stability or functionality.
8. **Documentation and Communication:**
   All changes and their outcomes must be documented, and relevant stakeholders must be informed of significant changes and their impacts.
9. **Review and Lessons Learned:**
   Post-implementation reviews should be conducted to assess the success of changes and identify areas for improvement in the change management process.

IT EQUIPMENT DECOMMISSIONING

Overview:
This manual outlines the procedures for decommissioning and disposing of IT equipment, focusing on secure data deletion, potential resale, and environmentally responsible disposal. It ensures the protection of sensitive data, responsible asset utilization, and compliance with environmental regulations.

Procedure:

1. **Scope:**
   Applies to all IT assets owned, managed, or maintained by Rogue Community College, including servers, workstations, network equipment, and associated storage devices.
2. **Inventory Management:**
   After data deletion and device cleaning, all decommissioned IT equipment must be identified and removed from the inventory list.

3. **Data Deletion:**
   All data stored on the equipment must be securely wiped to make sensitive and confidential data irretrievable, following industry best practices.
4. **Physical Destruction:**
   If secure data deletion is not feasible, physical destruction of the storage devices will be performed under supervision to ensure complete data destruction.
5. **Resale of Equipment:**
   If decommissioned equipment is functional and data has been securely removed, it may be sold through approved platforms, such as GovDeals, in compliance with local and national regulations.
6. **Environmentally Responsible Disposal:**
   Equipment unsuitable for resale must be disposed of responsibly, including recycling wherever possible and using certified e-waste organizations for disposal.
7. **Documentation:**
   All decommissioning procedures must be documented for audit purposes, including data deletion or destruction records.
8. **Roles and Responsibilities:**
   The IT Department is responsible for managing the decommissioning process. When retiring IT equipment, all employees must adhere to these guidelines.
9. **Compliance:**
   Failure to comply with these procedures could result in data breaches or regulatory violations. Any incidents of non-compliance must be reported to the IT Department.

SERVER AND IT EQUIPMENT MAINTENANCE AND UPDATE

Overview:
This manual outlines the procedures for maintaining and updating servers and IT equipment to ensure Rogue Community College's IT infrastructure's operational efficiency, security, and longevity.

Procedure:

1. **Scope:**
   Applies to all servers and IT equipment owned, managed, or operated by Rogue Community College.
2. **Regular Maintenance:**
   To maintain optimal working conditions, preventive maintenance must be conducted regularly on all servers and IT equipment. Maintenance should be scheduled at times that minimize disruption to college operations.

3. **Regular Updates:**
   Servers must be updated at least once a month. IT equipment should be regularly updated with patches released by manufacturers or developers to address vulnerabilities and improve performance.
4. **Testing:**
   Updates and patches must be tested in a controlled environment, such as a testing or staging server, before being applied to live systems to ensure they do not disrupt functionality.
5. **Hardware Upgrades:**
   Hardware components should be reviewed periodically for potential upgrades, especially when upgrades offer significant performance, security, or functionality improvements.
6. **Software Upgrades:**
   Outdated software poses security risks and functional limitations. Regular upgrades should be planned, and legacy systems should be phased out in an organized and timely manner.
7. **Documentation:**
   All maintenance activities, updates, patches, and upgrades must be documented for future reference and auditing purposes.
8. **Roles and Responsibilities:**
   The IT Department is responsible for planning, scheduling, and implementing all maintenance and update activities. Staff members must follow established schedules and procedures.
9. **Compliance:**
   Compliance with these guidelines is required to maintain the efficient operation and security of the College's IT systems. Any deviations must be reported to the IT Department.

VULNERABILITY TESTING GUIDELINES FOR SERVERS AND IT EQUIPMENT

Overview:
The Vulnerability Testing Manual at Rogue Community College (RCC) establishes protocols for regularly assessing the security of servers and IT equipment. This section is essential for identifying and mitigating vulnerabilities to protect RCC's IT assets and data's integrity, availability, and confidentiality.

Procedure:

1. **Scope:**
   This manual applies to all servers and IT equipment, both physical and virtual, under RCC's ownership, management, or operation. It ensures comprehensive security coverage across all IT infrastructure components.
2. **Annual Testing:**
   Vulnerability assessments are conducted annually on all servers and IT equipment. These assessments are vital in identifying potential security weaknesses and vulnerabilities that cyber threats could exploit.
3. **Testing Tools and Techniques:**
   Assessments utilize trusted tools and techniques following industry best practices. A combination of automated tools and manual inspection methods is recommended to ensure a thorough evaluation.
4. **Testing Environment:**
   Assessments are designed to minimize operational disruption and are typically conducted on replica systems, staging servers, or during periods of low activity. This approach helps maintain service availability.
5. **Mitigation and Remediation:**
   Once identified, vulnerabilities are classified based on potential impact and likelihood of exploitation. Remediation strategies are then developed and prioritized according to the severity of the vulnerabilities.
6. **Documentation:**
   Each stage of the assessment, from execution to findings and remediation actions, is carefully documented. This documentation serves as a resource for future assessments and audits, offering insights into the evolving threat landscape and the effectiveness of mitigation efforts.
7. **Roles and Responsibilities:**
   The RCC IT Department is responsible for conducting assessments and addressing identified vulnerabilities. All staff members are expected to cooperate with these procedures to ensure the security and integrity of RCC's IT systems.
8. **Compliance:**
   Compliance with these guidelines is required to maintain the security and functionality of the College's IT systems. Any deviations from the established procedures must be promptly reported to the IT Department.

IT DEPARTMENT STAFF POLICIES AND PROCEDURES

Overview:

The IT Department Staff Policies and Procedures at Rogue Community College (RCC) outline the

responsibilities, conduct, and performance guidelines for all IT Department staff. These policies ensure effective operations, uphold professional standards, and promote a positive work environment.

Procedure:

1. **Scope:**
   • Applies to all personnel in the IT Department at RCC.
   • Ensures uniform understanding and adherence to department policies.
2. **Roles and Responsibilities:**
   • Staff must fully understand and execute their specific roles and duties in alignment with RCC's mission and goals.
   • Regular role clarification sessions and duty assessments will ensure alignment with departmental objectives.
3. **Code of Conduct:**
   • Staff are expected to uphold high integrity, accountability, and respect standards.
   • Misconduct or unethical behavior is strictly prohibited.
   • Regular training on ethical practices and conduct guidelines will be provided.
4. **Data Privacy:**
   • Strict adherence to data privacy regulations and RCC policies is required when handling sensitive and confidential data.
   • Ongoing training on data privacy regulations and best practices will be provided.
5. **Training and Professional Development:**
   • Staff will participate in regular training and professional development to stay updated on technology trends and industry best practices.
   • Emphasis on continuous learning to enhance departmental capabilities and individual career growth.
6. **Communication:**
   • Clear, effective, and respectful communication within the department and across the College is essential.
   • Regular workshops will be conducted to improve communication skills and foster interdepartmental collaboration.
7. **Issue Resolution:**
   • Timely and constructive resolution of problems or conflicts is encouraged.
   • Clear channels for reporting and addressing issues within the department will be established.
8. **Performance Evaluation:**
   • Regular performance evaluations will provide constructive feedback and identify areas for improvement or professional development.

• The evaluation system will align with RCC's overall performance management framework.

9. **Security Compliance:**
   • Adherence to all RCC security policies and protocols is mandatory.
   • Regular security training sessions on password management, physical security, and protocol adherence will ensure the safety and integrity of IT resources.
10. **Yearly Continuing Education:**
    • All IT staff are required to engage in yearly continuing education to maintain and enhance professional skills.
    • Staff should refer to the "IT Staff Training Program" section of this document for details on available opportunities and guidelines.

END USER SUPPORT

Overview:

The End User Support section outlines the responsibilities and procedures for providing IT support services to the College's faculty, staff, and students. The goal is to ensure timely, efficient, and courteous assistance with IT-related issues, promoting an effective learning and teaching environment.

Procedure:

1. **Scope:**
   This section applies to the IT Department, specifically the End User Support team, and all end users of IT systems at Rogue Community College. It includes support for all hardware and software managed by the College.
2. **Support Channels:**
   End-user support is available through designated channels, including an IT service desk, email, telephone hotline, and self-service portals. These options allow users to communicate with the Support team directly for efficient issue resolution.
3. **Support Hours:**
   The End User Support team operates during regular business hours. After-hours support may be available for critical issues defined by separate service level agreements (SLAs). Requests for critical support outside regular hours should be made via the designated emergency contact method.
4. **Service Level Agreement (SLA):**
   Support requests will be addressed according to the SLA, which specifies response times, resolution times, and the availability of support services, providing end users with clear expectations.

5. **Prioritization:**
   Support requests are prioritized based on urgency and impact. A tiered priority system is used, with Level 1 representing the most critical issues affecting multiple users or disrupting essential operations.
6. **Training:**
   The IT Department provides training resources to help end users become self-sufficient in handling minor, non-critical issues. These resources include user manuals, FAQs, and troubleshooting guides.
7. **Feedback:**
   End-user feedback is encouraged to improve support services. Regular surveys and open feedback channels help the IT Department continuously enhance service quality.
8. **Roles and Responsibilities:**
   The End User Support team receives, classifies, resolves, or escalates support requests. They guide users through the resolution process, manage communication, and ensure user satisfaction.
9. **Documentation:**
   All support interactions must be documented in the service desk system. This includes the nature of the issue, steps taken to resolve it, user details, and resolution times. This documentation aids in future troubleshooting, reporting, and service improvement efforts.

IT NETWORK SERVICES

Overview:
The IT Network Services Manual provides guidelines for maintaining a reliable, secure, high-performing network infrastructure. This section is essential for ensuring the stability, availability, and efficient performance of network services that support the college's teaching, learning, research, and administrative functions.

Procedure:

1. **Scope:**
   This section applies to the IT Department, specifically the Network Services team, and covers all network-related hardware, software, and communication technologies owned, managed, or leased by the College. This includes routers, switches, firewalls, wireless access points, network cabling, and related equipment.
2. **Network Design and Configuration:**
   The Network Services team is responsible for designing and configuring the network infrastructure according to industry best practices and standards. This involves planning

for scalability to accommodate growth and incorporating redundancy to ensure business continuity and minimize downtime.

3. **Network Security:**
   A multi-layered approach to network security is required, incorporating firewalls, intrusion detection/prevention systems, secure access controls, and encryption where necessary. Regular security audits must be conducted to identify vulnerabilities and ensure adequate security measures are in place.
4. **Access Management:**
   Network access should follow the least-privilege principle, granting only the necessary access to specific network resources based on individual roles and responsibilities. Access rights should be regularly reviewed, updated, and immediately revoked when no longer needed.
5. **Performance Monitoring:**
   Continuous monitoring of network performance is essential to ensure optimal operation. This includes tracking network traffic patterns, bandwidth usage, latency, and error rates. Monitoring tools should provide real-time alerts of potential issues, enabling proactive troubleshooting and resolution.
6. **Maintenance and Upgrades:**
   The Network Services team should carry out regular maintenance activities, including software updates, hardware upgrades, and the replacement of end-of-life equipment. Major network changes or upgrades should be scheduled during off-peak hours and communicated in advance to minimize disruptions.
7. **Backup and Disaster Recovery:**
   Backup procedures should regularly capture network configurations and critical network data. A comprehensive disaster recovery plan should be developed, routinely updated, and tested to ensure rapid restoration of network services in case of failure or other catastrophic events.
8. **Incident Management:**
   The Network Services team is responsible for promptly responding to and managing network incidents. All incidents should be logged and analyzed for root causes, and lessons learned should be incorporated into future network operation procedures.
9. **Compliance:**
   Full compliance with applicable legal and regulatory requirements, contractual obligations, and internal college policies related to network services is mandatory. This includes data privacy regulations, copyright laws, and software licensing terms.

CLOSURE PLAN FOR IT SECURITY ALERTS

Overview:

The Closure Plan for IT Security Alerts at Rogue Community College ensures a robust response to critical security alerts from Sophos MDR and Microsoft Defender during periods when the college is officially closed. This plan outlines responsibilities and procedures for addressing alerts to maintain the security and integrity of RCC's IT infrastructure.

Procedure:

1. **Responsibility During Closure Days:**
    - The IT Leadership team is the primary responder for Sophos MDR and Microsoft Defender alerts during closure days.
    - They will monitor and assess the alerts to determine the severity and the necessary course of action.
2. **Escalation and Staff Callback:**
    - If an alert requires immediate attention beyond the capabilities of the IT Leadership team, IT staff will be called back to address the issue.
    - The decision to call back IT staff will be based on the nature and severity of the alert.
3. **Compensation for IT Staff:**
    - IT staff called back to address security alerts during closure periods will receive compensation in line with college policies.
    - The compensation mechanism will follow established college policies for emergency or overtime work.
4. **Communication Protocol:**
    - A clear communication protocol will be in place to ensure timely and efficient mobilization of IT staff during closures.
    - IT staff will have access to necessary contact details and emergency response procedures.
5. **Training and Preparedness:**
    - The IT Leadership team and relevant IT staff will receive regular training on responding to security alerts from Sophos MDR and Microsoft Defender.
    - Preparedness drills may be conducted to ensure readiness for incident response during closure periods.
6. **Documentation and Reporting:**
    - All security incidents and response actions during closure periods will be thoroughly documented.
    - Post-incident reports will be compiled and reviewed to refine response strategies and update protocols.
7. **Review and Updates:**

- This Closure Plan will be reviewed regularly to ensure its effectiveness and alignment with current security landscapes and college policies.
- The plan will be updated as necessary to respond to changes in technology, threat patterns, or college operational procedures.

IT RISK MANAGEMENT

Overview:
The IT Risk Management section outlines principles and procedures for identifying, assessing, treating, and continuously monitoring risks associated with information technology that could impact the College's operations, reputation, or the security of its information assets. Proactive risk management helps protect critical infrastructure, maintains data confidentiality, integrity, and availability, and supports the College's strategic objectives.

Procedure:

1. **Scope:**
   This section applies to all members of the IT Department and users of the College's IT resources, covering all systems, processes, data, and IT-related activities. This includes on-premise and cloud-based systems, software, hardware, data, and networks owned, managed, or used by the College.

2. **Risk Management Framework:**
   A formal, structured risk management framework must govern all IT risk management activities, aligned with industry best practices such as ISO 31000 (Risk Management) and ISO 27005 (Information Security Risk Management).

3. **Risk Identification:**
   Risks should be identified through self-assessments, third-party audits, threat and vulnerability assessments, penetration tests, security incident reports, and user feedback. The process should account for potential threats, vulnerabilities, and impacts on information assets' confidentiality, integrity, and availability.

4. **Risk Assessment:**
   Each identified risk should be assessed based on its potential impact and likelihood. Impact assessments should consider quantitative factors (financial loss, downtime) and qualitative factors (reputational damage, regulatory non-compliance). Risks should be categorized as low, medium, or high to guide risk treatment efforts.

5. **Risk Treatment:**
   Appropriate strategies should be selected based on the risk assessment, such as risk acceptance (tolerating the risk), risk avoidance (discontinuing the risky activity), risk

mitigation (implementing controls), or risk transfer (sharing or outsourcing the risk). The chosen strategy must align with the College's risk appetite and tolerance levels.

6. **Risk Monitoring and Review:**
   IT risks should be continuously monitored, with regular reviews and updates to reflect changes in the IT environment, business objectives, or threat landscape. Audits and reviews should validate the effectiveness of risk treatments and identify any emerging risks.

7. **Risk Reporting:**
   The IT department, senior management, and other stakeholders should receive regular reports on IT risks, treatment status, and the effectiveness of strategies. This will support decision-making, strategic planning, and organizational awareness of significant IT risks.

8. **Roles and Responsibilities:**
   The IT Department is responsible for implementing this section, executing risk management activities, and coordinating these efforts across the College. All IT users must comply with this manual, support risk management activities, and report potential risks to the IT Department.

9. **Training and Awareness:**
   Regular training and awareness programs should be conducted to ensure all IT users understand their role in managing IT risks and are familiar with risk management policies and procedures.

IT PRIVACY STATEMENT

Overview:
The IT Privacy Manual ensures the integrity and confidentiality of personal information managed by the College's IT systems. It outlines how personal data is collected, stored, used, disclosed, and safeguarded in compliance with data protection regulations. The goal is to respect individual privacy, protect personal information from unauthorized access and misuse, and ensure compliance with relevant laws.

Procedure:

1. **Scope:**
   This section applies to all information systems, services, procedures, and activities involving personal information collection, processing, storage, transmission, or disposal. It applies to all IT department personnel and users of the College's IT resources, regardless of role or position.

2. **Data Collection:**
   Personal data will only be collected for legitimate purposes aligned with the College's functions and activities. Data collection will be transparent, and users will be informed of the purposes for which their data is being collected. Only the minimum necessary personal information will be collected, adhering to data minimization and purpose limitation principles.

3. **Data Use:**
   Personal information will be used solely for the purposes for which it was collected or for other legal purposes expressly agreed to by the individual or required by law. Any changes in data use will be communicated to the individual, and their consent will be sought when necessary.

4. **Data Disclosure:**
   Personally identifiable information will not be shared with third parties without explicit consent unless required by law or necessary to provide a requested service. All disclosures will be documented and secured to prevent unauthorized access or data breaches.

5. **Data Access and Correction:**
   Individuals have the right to access their personal information held by the College and request corrections or deletions to ensure accuracy, completeness, and relevance. Clear mechanisms for handling such requests will be in place and communicated to users.

6. **Data Security:**
   Strong security measures, such as encryption, access controls, and secure network architectures, will be employed to protect personal information from unauthorized access, alteration, disclosure, or destruction. Security measures will be proportional to the sensitivity of the data and the risks of a privacy breach.

7. **Data Retention and Disposal:**
   Personal information will be retained only as long as necessary for its intended purpose or as required by law. Once no longer needed, the data will be securely and effectively disposed of to prevent unauthorized access or recovery.

8. **Privacy Impact Assessment:**
   Any new or significantly revised IT system or service that handles personal information will undergo a privacy impact assessment (PIA). The PIA will help identify and mitigate potential privacy risks, ensuring continued compliance with privacy regulations.

9. **Training and Awareness:**
   Regular privacy training and awareness programs will be conducted to ensure that all IT users understand their responsibilities in protecting personal data. The training will address data protection principles, privacy rights, risks, and protective measures.

10. **Compliance:**
    Adherence to this section and all applicable privacy laws and regulations is mandatory. Non-compliance may result in disciplinary action, up to and including termination, as well as potential legal penalties.

ROGUE COMMUNITY COLLEGE IT STAFF TRAINING PROGRAM

Program Overview:
The IT Staff Training Program is designed to enhance the skills and knowledge of IT personnel, keeping them up-to-date with the latest technologies, trends, and best practices in the field. The program fosters continuous professional development to ensure IT staff can effectively support the College's technology needs.

Scope:
This program applies to all IT department members, including full-time, part-time, temporary, and contract staff.

Program Components:

1. **Training Needs Assessment:**
   Regular assessments will be conducted to identify each IT staff member's training needs based on their current roles, career goals, and the IT department's strategic objectives.
2. **Technical Training:**
   Training on specific technologies, tools, or systems used by the College. This may include server management, network administration, cloud computing, cybersecurity, data analytics, and more.
3. **Certification Programs:**
   Staff are encouraged to pursue relevant professional certifications such as CompTIA A+, Network+, Security+, Microsoft Certified: Azure Solutions Architect Expert, AWS Certified Solutions Architect, and Certified Information Systems Security Professional (CISSP). The College supports staff in preparing for these certifications.
4. **Soft Skills Training:**
   Training will also focus on soft skills such as communication, teamwork, leadership, project management, and customer service. These skills are essential for effective collaboration and service delivery.
5. **Security Awareness Training:**
   Regular security awareness training will be provided to keep IT staff informed about the latest cybersecurity threats and best practices for securing systems and data.

6. **Vendor-Specific Training:**
   Vendors may provide specific training when new systems or technologies are implemented to ensure IT staff can effectively deploy and manage their products.
7. **On-the-Job Training:**
   On-the-job training will be offered through daily work activities under the guidance of experienced staff or supervisors, allowing staff to apply and reinforce their learning.
8. **Yearly Continuing Education:**
   - All IT staff are required to engage in yearly continuing education to maintain and enhance their professional skills.
   - This includes workshops, seminars, online courses, or obtaining relevant IT and cybersecurity certifications.
   - Training activities are aligned with current industry trends and the evolving needs of the College's IT infrastructure.
   - Staff members are encouraged to share their newly acquired knowledge with colleagues, promoting a culture of continuous learning.

Training Methods:
Training will be delivered through various methods, such as in-person workshops, online courses, webinars, self-study, and conferences. The technique used will depend on the nature of the training, staff availability, and resources.

Program Evaluation:
The effectiveness of the Training Program will be evaluated regularly through feedback surveys, tests, performance reviews, and assessments of IT operations within the College.

Continuous Learning Culture:
This program reflects the College's commitment to fostering a continuous learning and improvement culture within the IT department. Staff are encouraged to pursue professional development, share knowledge with colleagues, and apply their learning to enhance IT services and operations.
By participating in this program, IT staff will be better equipped to support the College's technology needs, ultimately improving IT performance, security, and service delivery.