RAMAPO COLLEGE OF NEW JERSEY

411A: Cybersecurity Protocols & Compliance Manual (CPCM)

Supplemental Resource to Policy 411: Cybersecurity

October 2025

TABLE OF CONTENTS

I. INTRODUCTION

In accordance with Ramapo College of New Jersey Policy & Procedure 411: Cybersecurity, the importance of cybersecurity cannot be overstated. Ramapo College, hereafter “the College”, recognizes that safeguarding the integrity, confidentiality, and availability of its digital assets and sensitive information is not only essential but also integral to its mission as an institution of higher learning. Cybersecurity is not merely a technical concern; it is a fundamental responsibility that impacts every facet of our college community.

The reliance on technology for teaching, learning, research, administrative operations, and communication has grown significantly. While this digital transformation offers countless benefits, it also exposes us to a wide range of cybersecurity threats and vulnerabilities. The consequences of a cybersecurity breach can extend far beyond financial loss; they can affect our reputation, compromise the privacy of individuals, and disrupt the academic and administrative functions that are the lifeblood of Ramapo College.

This comprehensive Cybersecurity Protocols & Compliance Manual, hereafter “CPCM”, was developed as a testament to our commitment to securing our digital environment, recognizing that cybersecurity is a shared responsibility involving the entire Ramapo College community. It provides a structured framework to mitigate risks, protect sensitive data, and establish a culture of vigilance and responsibility among our staff, faculty, students, and partners. In addition, this policy serves as a guiding document for the college community, outlining the principles and practices necessary to create a secure and resilient cybersecurity posture. By adhering to the principles and practices outlined in Policy and Procedure 411 and this CPCM, we ensure not only the protection of our digital assets but also the continued growth and success of Ramapo College.

II. KEY OBJECTIVES

- Protection of Sensitive Data
    - Ramapo College recognizes the critical importance of safeguarding sensitive data, including but not limited to student records, employee information, financial data, and research findings. The CPCM aims to:
        - Implement robust data classification and handling procedures to identify and protect sensitive data appropriately.
        - Ensure that sensitive data is encrypted both in transit and at rest to prevent unauthorized access or data breaches.
        - Establish strict access controls to restrict data access to authorized personnel only.
- Network Security

  - In today's interconnected environment, a secure network is paramount to the college's operations and data protection. This policy seeks to:
    - Define network security measures, including firewall configurations, intrusion detection/prevention systems, and continuous monitoring.
    - Promote regular network vulnerability assessments and penetration testing to identify and mitigate potential weaknesses.
    - Require the use of Virtual Private Networks (VPNs) for secure remote access to the college's network resources.
- Compliance with Legal and Regulatory Requirements
  - Ramapo College is committed to complying with all relevant cybersecurity regulations and frameworks, including the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Payment Card Industry Data Security Standard (PCI-DSS), and the Gramm-Leach-Bliley Act (GLBA). The CPCM aims to:
    - Establish a framework for aligning cybersecurity practices with NIST CSF guidelines to improve overall cybersecurity resilience.
    - Ensure that GLBA requirements related to the protection of financial information are met, including data security, risk assessments, and customer privacy.
    - Along with Business Services, ensure compliance with PCI-DSS by reviewing credit card terminals and online payment sites, if any, to verify secure handling, storage, and transmission of cardholder data.
    - Annually review and update the CPCM to remain in compliance with evolving legal and regulatory requirements in the cybersecurity landscape.

By articulating these objectives, the CPCM underscores the commitment of Ramapo College to proactively address cybersecurity challenges. The College recognizes that cybersecurity is not a static endeavor but an ongoing process requiring vigilance, education, and collaboration across the entire institution.

III. Scope

Ramapo College Policy and Procedure 411: Cybersecurity, and the CPCM encompass all systems, personnel, and data within the purview of Ramapo College. It is imperative that every facet of our institution is covered to ensure the comprehensive protection and security of our digital assets. The scope of these Cybersecurity resources includes but is not limited to:

1. Systems: The CPCM applies to all computer systems, servers, workstations, network devices, mobile devices, and any other hardware or software components that are part of Ramapo College's information technology infrastructure.
2. Personnel: All individuals who are part of the Ramapo College community, including employees, contractors, consultants, vendors, students, and any other authorized users,

are subject to the provisions outlined in this policy. It is the responsibility of all personnel to adhere to the CPCM guidelines and best practices.

3. Data: The CPCM is designed to protect all types of data stored, processed, or transmitted by Ramapo College. This includes, but is not limited to:
    a. Student records and academic information
    b. Employee records and personnel data
    c. Financial and budgetary information
    d. Research data and intellectual property
    e. Institutional documents and communications
    f. Any other data deemed sensitive or critical to the college's operations and mission

The comprehensive scope of the CPCM ensures that cybersecurity measures are applied consistently across all aspects of Ramapo College's digital environment. By covering systems, personnel, and data comprehensively, we aim to minimize risks, safeguard sensitive information, and create a secure and resilient cybersecurity posture for the entire college community.

IV. Roles and Responsibilities

1. **Chief Information Officer (CIO),** The CIO is the highest-ranking individual responsible for cybersecurity within Ramapo College. Their primary responsibilities include:

    - Developing and implementing the college's cybersecurity strategy and policies.
    - Overseeing cybersecurity risk management and compliance efforts.
    - Coordinating incident response and recovery efforts.
    - Ensuring that cybersecurity practices align with industry standards and regulatory requirements.
    - Communicating cybersecurity priorities and updates to senior management and the college community.

2. **Information Security Team - Deputy Chief Information Officer, Virtual Chief Information Security Officer (VCISO):** The Information Security Team, led by the Deputy CIO, consists of security professionals responsible for executing the cybersecurity strategy. Key responsibilities include:

    - Conducting regular security assessments, risk assessments, and vulnerability management.
    - Monitoring and responding to security incidents and threats.
    - Managing access controls and user permissions.

- Implementing security technologies and best practices.
- Providing cybersecurity training and awareness programs.

3. **System Administrators:** System administrators play a critical role in maintaining the security of college systems. Their responsibilities include:
    - Ensuring that systems are properly configured, patched, and updated.
    - Implementing security controls and policies on systems.
    - Conducting regular system audits and monitoring for anomalies.
    - Managing user accounts and access permissions.
    - Assisting in incident response and recovery efforts.
4. **End-Users:** All members of the college community, including employees, students, faculty, and authorized users, have a role in maintaining cybersecurity. Their responsibilities include:
    - Following cybersecurity policies, protocols, and best practices.
    - Using strong, unique passwords and enabling multi-factor authentication where applicable.
    - Reporting security incidents or suspicious activities promptly.
    - Avoiding risky behavior, such as clicking on suspicious links or downloading unknown files.
    - Participating in cybersecurity training and awareness programs.
5. **Management and Leadership:** Senior management and leadership across the college also play a critical role in cybersecurity. Their responsibilities include:
    - Providing support and resources for cybersecurity initiatives.
    - Ensuring that cybersecurity is integrated into strategic planning and decision-making.
    - Approving cybersecurity budgets and resource allocation.
    - Promoting a culture of cybersecurity awareness and accountability.
    - Being informed and proactive in addressing cybersecurity risks.
6. IT Compliance Officer: The IT Compliance Officer ensures IT policies and controls meet regulations and institutional standards. Their responsibilities include:

- Ensuring IT policies and controls align with laws, regulations (e.g., GLBA, NIST), and institutional standards.
- Collaborating with the Internal Auditor and Information Security Team to identify, assess, and address IT security and compliance risks.
- Assisting with internal audits, responding to compliance findings, and ensuring corrective actions are implemented effectively.

These roles collectively contribute to the effective implementation of cybersecurity measures at Ramapo College. Clear delineation of responsibilities ensures that each stakeholder understands their role in maintaining the security and integrity of the college's digital assets and information. Additionally, regular communication and collaboration among these roles are vital to creating a robust cybersecurity posture.

V. Security Awareness and Training

The college’s cybersecurity training program educates all employees about potential threats and best practices. Employees are required to report security incidents, and the training program provides clear procedures for doing so. Training is conducted using interactive web-based training, which is required to be completed by the Ramapo community both monthly and annually.

VI. Access Controls

Access control protocols are crucial to ensure that only authorized personnel have access to systems and data within Ramapo College. These protocols help safeguard against unauthorized access, data breaches, and protect the confidentiality, integrity, and availability of sensitive information. Ramapo aligns with NIST 800-63B compliance standards for digital identity guidelines. The following are key components of access control protocols:

1. **User Authentication:**
    - All users must authenticate themselves before accessing systems or data. This includes providing a unique username and a strong, confidential password.
    - Passwords must meet complexity requirements, such as minimum length, a mix of upper and lower case letters, numbers, and special characters.
    - Passwords must never be shared, even between assistants and their managers.
2. **Multi-Factor Authentication (MFA):**
    - MFA is implemented for sensitive systems and applications. It requires users to provide two or more forms of authentication before gaining access. These factors typically include something the user knows (password), something the user has

(a mobile app or token), or something the user is (biometric data like fingerprint or facial recognition).

- MFA enhances security significantly by adding an additional layer of protection, even if the password is compromised.

3. **Role-Based Access Control (RBAC):**

   - RBAC ensures that users have access only to the resources and data necessary for their roles and responsibilities following a least privilege model, or the principle of minimizing unnecessary permissions.
   - User roles and permissions are regularly reviewed to align with changes in job responsibilities.

4. **Access Requests and Approval:**

   - A formal process exists for requesting access to systems and data, which includes the approval of appropriate supervisors or data owners/stewards.
   - Records of access requests and approvals for auditing purposes are maintained.

5. **Access Revocation:**

   - Protocols including a notification to the ITS Help Desk or automated notices for employment separations, followed by a series of system and audit procedures, exist for promptly revoking access when employees change roles, leave the college, or no longer require access to specific systems or data.

6. **Audit Trails and Monitoring:**

   - System audit trails and monitoring systems track user activities and access to sensitive data.
   - Logs generated both manually and via log aggregation systems are regularly reviewed for suspicious activities and unauthorized access attempts.

7. **Physical Access Control:**

   - Physical access to server rooms, data centers, and critical infrastructure to prevent unauthorized entry are secured.
   - Access control mechanisms such as biometric scanners or card readers for restricted areas have been implemented.

8. **Regular Access Reviews:**

- Periodic access reviews and audits are conducted to ensure that users have the appropriate level of access.
- Unnecessary access rights are promptly removed.

By implementing these access control protocols and practices, Ramapo College can significantly reduce the risk of unauthorized access to sensitive systems and data, protect against insider threats, and enhance overall cybersecurity.

VII. Procedures for Encrypting and Protecting Sensitive Data

Sensitive data, both in transit and at rest, are encrypted and the security and confidentiality of information at Ramapo College are maintained. This is achieved via:

1. Encryption in Transit:

- Current versions of Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols are used for encrypting data transmitted over networks. Ensure that these protocols are implemented and properly configured for all network communication, especially for web-based applications and email.
- For email communications, email encryption protocols, such as STARTTLS (a protocol commonly used in SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), and POP3 (Post Office Protocol) to enhance security) or end-to-end encryption, are enabled to protect the confidentiality of email content during transmission.

2. Encryption at Rest:

- Encryption at rest is enabled for all storage systems and backup solutions used across the college.
- Encryption occurs at the file level or disk level, depending on the specific capabilities of the storage and backup systems in use.
- Encryption keys are stored securely, separate from the data they protect, and follow best practices for key management.

3. Immutable Backups on Cloud Storage:

Immutable backups on a cloud storage platform exist to help protect against data deletion or modification, ensuring data integrity. S3 buckets are configured with the Object Lock feature to prevent data from being deleted or modified for a specified retention period.

4. Data Classification and Handling:

- A clear data classification framework based on the sensitivity and criticality of data is used to classify data into categories such as Low Risk Data, Moderate Risk Data, and High Risk Data as defined in the RCNJ IT Policy 410: Data Protection (PII).
- Access controls and permissions are defined based on data classification. Only authorized personnel have access to sensitive data.
- Data handling procedures include:
    - Using encryption as appropriate, based on the classification.
    - Limiting data transfer to authorized devices and networks.
    - Monitoring and auditing access to sensitive data.
    - Implementing secure deletion or destruction methods when data is no longer needed.

5. Data Backup and Recovery:

- Data backups are automated, scheduled regularly, and tested for data integrity and recoverability.
- Backup retention policies exist, taking into account regulatory requirements and the sensitivity of the data.
- Backups are stored securely, with access controls and encryption applied, both in transit and at rest.

6. Ongoing Monitoring and Compliance:

- Includes regularly monitoring and assessing the effectiveness of encryption, data classification, and handling procedures.
- Audits and security assessments are performed annually to verify compliance with these procedures and identify areas for improvement, such as ensuring system updates and following best practices related to data encryption and protection.

By implementing these procedures, Ramapo College establishes a strong foundation for data protection and compliance with regulatory requirements while utilizing on premises and cloud services for storage, backup, and immutable data. Data encryption, classification, and handling are vital components of a robust cybersecurity posture.

VIII. Network Security

Ensuring robust network security is critical for protecting Ramapo College's digital assets and sensitive information. Here are detailed network security measures, including firewall rules, endpoint detection systems, and regular network vulnerability assessments, that the college currently has set in place:

1. Firewall Rules:

- **Firewall Configuration:** Stateful firewalls, which are security devices that monitor and filter network traffic based on the state of active connections, at the network perimeter and between network segments have been implemented. Configure firewall rules to permit necessary traffic and deny all other traffic by default.
- **Application Layer Filtering:** Deep packet inspection and application-layer filtering are applied to identify and block malicious content and known attack vectors.
- **Regular Firewall Rule Review:** Periodic reviews of firewall rules are completed to ensure they align with business needs and security policies. Remove or modify rules that are no longer necessary or pose potential risks.

2. Endpoint Detection and Response (EDR): The College utilizes an EDR solution, deployed across laptops, desktops, and servers, including office workstations and classroom labs. EDR is a critical cybersecurity tool that monitors, detects, investigates, and responds to threats targeting endpoints.

Key features of the College's EDR solution include:

- Anomaly Detection: Identifies deviations from normal behavior to detect advanced threats, such as zero-day attacks and advanced persistent threats (APTs).
- Real-Time Alerts: Provides detailed notifications of suspicious activities, enabling rapid threat assessment and response.
- Automated Response: Isolates infected endpoints, terminates malicious processes, and restores endpoints to a secure state to minimize attack impact.

The EDR solution integrates with the College's incident response process, ensuring a structured approach to threat management:

1. Initial Triage: Assess and prioritize alerts.
2. Investigation: Analyze endpoint data to determine the scope of the threat.
3. Containment and Neutralization: Prevent further spread and neutralize the threat.
4. Remediation: Eliminate the threat and restore systems.

5. Post-Incident Analysis: Review and improve security measures.

This comprehensive approach strengthens the College’s defense against sophisticated cyber threats.

3. Regular Network Vulnerability Assessments:

- **Scheduled Scans:** Regular vulnerability assessments are conducted using automated scanning tools to identify weaknesses in the network, systems, and applications.
- **Patch Management:** Vulnerabilities are prioritized based on their severity and potential impact. A comprehensive patch management program has been developed to remediate identified vulnerabilities promptly.
- **Penetration Testing:** Penetration testing is generally done annually (when funds allow) to simulate real-world attacks and evaluate the effectiveness of security measures.

4. Virtual Private Networks (VPNs) for Remote Access:

- **VPN Implementation:** All employees, contractors, and authorized users are required to utilize VPNs when accessing college resources remotely.
- **Strong Authentication:** Multi-factor authentication (MFA) is required for VPN access to enhance security.
- **Logging and Monitoring:** VPN connections are logged and monitored for unusual or unauthorized access attempts.
- **Regular Updates:** VPN software and configurations are regularly maintained and kept up to date to patch vulnerabilities and maintain security.

5. Security Policy Enforcement:

- **Enforce Network Security Policies:** Refer to the Information Security Policy and the Acceptable Use Policy, as they govern network security, including remote access policies and firewall policies. Certain software containing anomaly detection will automatically search for violations of these policies. Other incidents are via awareness, the College’s managed security operations center (SOC), and reporting. Violations of any security policies can result in termination or suspension of network resources and will be reported to the appropriate disciplinary entity.
- **User Education:** Users are continuously educated about the importance of network security, VPN usage, and safe remote access practices.

6. Network Segmentation:

- **Segment Sensitive Data:** Network is segregated into segments to isolate sensitive data from less critical areas, limiting the potential for lateral movement by attackers.
- **Access Control Lists (ACLs):** ACLs and Virtual Local Area Networks (VLANs) have been implemented to control traffic flow and restrict access between network segments.

7. Incident Response Planning:

- The ITS team developed an Incident Response Plan (IRP), which is tested and reviewed annually, to outline the steps to take in the event of a network security breach.
- Within the IRP, roles and responsibilities are defined for incident response team members.
- The IRP includes clear procedures for containment, eradication, recovery, and communication during security incidents.

By implementing these network security measures, Ramapo College can significantly reduce the risk of security breaches, protect sensitive data, and maintain the integrity of its digital infrastructure.

IX. Incident Response Plan

In concert with the Ramapo College Emergency Preparedness Plan, the Ramapo College Incident Response Plan (IRP) outlines the procedures to be followed in the event of a cybersecurity incident. A cybersecurity incident is defined as any event that compromises the confidentiality, integrity, or availability of the college's digital assets or sensitive information. This IRP aims to minimize the impact of incidents, protect the college's reputation, and ensure the swift recovery of affected systems and data.

The full details of Ramapo College's Incident Response Plan are outlined in the RCNJ IT Incident Response Plan document which, due to the document sensitivity, can only be obtained through ITS Leadership.

X. Patch Management

Regular Patch Management and System Updates Process: Effective patch management is essential for addressing known vulnerabilities and ensuring the security of Ramapo College's digital infrastructure. For on-premise systems, patch management is overseen by the relevant ITS team with expertise in the specific system. Cloud systems and applications are patched by their respective vendors. However, some systems may involve additional costs for version updates, making their management more complex. All other systems are updated and maintained by the technical administrators in the respective departments responsible for that software.

The following process outlines how ITS manages patches and system updates efficiently:

1. Patch Identification:

- Use automated tools to scan systems and applications for missing patches and vulnerabilities.
- Prioritize patches based on their severity, potential impact, and relevance to the college's environment.

2. Patch Testing:

- Use a testing environment that replicates the college's production systems as closely as possible.
- Test patches and updates thoroughly in the isolated environment to ensure they do not cause compatibility issues or disrupt critical operations.
- Create a testing checklist that includes functional, security, and performance testing criteria.

3. Change Management:

- Integrate the patch management process with the ITS' change management protocols to ensure proper documentation, approval, and tracking of patch deployment.
- Obtain approval from relevant stakeholders before deploying patches to production systems.
- Refer to the ITS Change Management Protocol document for comprehensive details.

4. Patch Deployment:

- Schedule regular maintenance windows during off-peak hours to minimize disruption to college operations.
- Deploy patches to production systems following the predetermined schedule.
- Automate patch deployment when possible to ensure timely updates and reduce CPCM errors.

5. Rollback Plan:

- Develop a rollback plan in case a patch causes unexpected issues or disruptions.
- Ensure that the rollback plan is well-documented and tested in the testing environment.

6. Monitoring and Verification:

- Continuously monitor systems after patch deployment to ensure they are functioning correctly and securely.
- Verify that patches have been applied successfully and vulnerabilities have been addressed.

7. Reporting and Documentation:

- Maintain detailed records of all patch management activities, including patch identification, testing results, deployment schedules, and verification.
- Document any issues encountered during the patching process and their resolutions.

8. Patch Management Tools:

- Utilize dedicated patch management tools or software to automate and streamline the patch management process.
- Ensure that these tools provide real-time reporting and status updates on patch deployment.

9. Third-Party Software and Dependencies:

- Include third-party software, applications, and dependencies in the patch management process. Ensure they are updated in a timely manner.
- Collaborate with vendors to receive notifications and patches for third-party software used by the college.

10. Ongoing Monitoring and Updates:

- Maintain an ongoing cycle of monitoring, testing, and deploying patches to address emerging vulnerabilities.
- Regularly review and update the patch management process to align with evolving security requirements and best practices

XI. Auditing, Security Monitoring, and Logging

Use of Security Information and Event Management (SIEM) Systems with a SOC and EDR:

Ramapo College utilizes Security Information and Event Management (SIEM) systems, including BitSight, in conjunction with a Security Operations Center (SOC) and an Endpoint Detection and Response (EDR) solution to comprehensively monitor and log all network and system activities. This integrated approach enhances the college's cybersecurity posture and incident response capabilities. Here's how these components work together:

1. Logging and Monitoring:

- BitSight is configured to collect and analyze logs from various network and system components, including firewalls, servers, applications, and network devices.
- Real-time log monitoring, whether automated, human-triggered, or human-in-the-loop, enables the detection of security events, anomalies, and potential threats.

2. Centralized Log Storage:

- Logs generated by different systems and devices are centralized in the SIEM systems, providing a unified view of network and system activities.
- Centralized storage ensures that logs are tamper-evident and readily accessible for analysis and reporting.

3. Retention Periods:

- Retention periods for logs are defined based on regulatory requirements, legal obligations, and the college's internal policies. Common retention periods for different log types include:
  - Security event logs: Typically retained for at least 1 year.
  - System logs: Retained for a minimum of 90 days.
  - Access logs: Retained for at least 180 days.
- Automated log archiving and rotation have been configured to ensure compliance with retention policies.

4. Log Analysis and Procedures:

- Procedure includes analyzing logs within the SIEM systems, SOC, and EDR to detect security incidents, anomalies, and potential threats.
- Predefined correlation rules and custom queries are used to identify suspicious patterns and behaviors.
- There are alerting mechanisms in place, which notify the SOC and incident response team when critical security events are detected.

5. SOC and EDR Integration:

- The SOC is responsible for monitoring and analyzing security events and alerts generated by the SIEM systems, EDR, and other security tools.
- EDR solutions are deployed on endpoints (e.g., workstations and servers) to provide real-time threat detection, investigation, and response capabilities.
- The SOC collaborates with the EDR team to investigate and respond to endpoint-related security incidents.

6. Incident Response:

- Integrated within the IRP is the SIEM systems, SOC, and EDR to facilitate rapid incident detection and response.
- Workflows and procedures for responding to security incidents are established based on the information gathered from log analysis, SOC alerts, and EDR investigations.

7. Regular Review and Updates:

- Annually review and update log analysis procedures, correlation rules, and alerting thresholds to adapt to evolving threats and vulnerabilities.
- Regular training for staff responsible includes training on log analysis, SOC operations, and EDR management to ensure these staff members are equipped to identify and respond to security incidents effectively.

8. Compliance and Reporting:

- Compliance reports and audit trails are generated from SIEM data to demonstrate adherence to regulatory requirements and internal policies.
- Records of all log analysis activities, SOC operations, and EDR investigations for compliance and reporting purposes are maintained.

By integrating SIEM systems, a SOC, and an EDR solution, Ramapo College enhances its ability to monitor and respond to security events across its network, endpoints, and systems. This multi-layered approach ensures a proactive and comprehensive cybersecurity defense strategy.

XII. VENDOR MANAGEMENT

Addressing Third-Party Cybersecurity Risks with Vendor Assessment and Monitoring:

Ramapo College recognizes the importance of managing third-party cybersecurity risks effectively. To establish a robust framework for vendor assessment and monitoring, the college utilizes BitSight for continuous monitoring and adheres to the following procedures:

1. Vendor Assessment and Due Diligence:

- Before engaging with a third-party vendor, Ramapo College conducts a thorough assessment to evaluate the vendor's cybersecurity posture.
- Assessments include a review of the vendor's security policies, practices, and compliance with cybersecurity standards and best practices.

2. Vendor Selection Criteria:

- Criteria for selecting vendors consider their cybersecurity practices, including their ability to protect sensitive data and maintain the confidentiality, integrity, and availability of college information.

3. Vendor Contractual Requirements:

- Vendor contracts and agreements include specific cybersecurity clauses and requirements. These requirements mandate that vendors adhere to established cybersecurity standards and best practices throughout their engagement with the college.
- Contracts also stipulate reporting obligations in the event of security incidents or breaches involving the vendor's systems or services.
- RCNJ Purchase Order Terms & Conditions now include terms requiring vendors to maintain the confidentiality and security of the College’s information in compliance with Gramm-Leach-Bliley Act (GLBA), notify the College of any security incidents, and allow the College to audit its security practices for compliance with the GLBA Safeguards Rule.

4. Continuous Vendor Monitoring:

- Ramapo College uses BitSight for continuous monitoring of third-party vendors' cybersecurity performance.
- BitSight provides ongoing security ratings and insights into vendors' vulnerabilities, data breaches, and security hygiene.

5. Vendor Security Improvement Plans:

- In cases where vendors' security ratings fall below acceptable thresholds, Ramapo College collaborates with vendors to develop and implement security improvement plans.
- These plans outline specific remediation actions and timelines for improving security practices.

6. Vendor Compliance Audits:

- The College ensures vendor compliance with cybersecurity standards and contractual requirements by including clauses in purchase order terms and conditions, requiring vendors to comply with the Gramm-Leach-Bliley Act (GLBA), and by monitoring vendor BitSight scores. Monitoring BitSight scores helps assess the effectiveness of the vendor's security controls and practices.

7. Incident Response Collaboration:

- Ramapo College maintains clear communication and collaboration channels with vendors in the event of a security incident.
- Vendors are expected to promptly report any security incidents or data breaches that may impact college data or systems.

8. Security Standards and Best Practices:

- Ramapo College mandates that vendors adhere to recognized cybersecurity standards and best practices, such as NIST Cybersecurity Framework, ISO 27001, the Gramm-Leach-Bliley Act (GLBA), and CIS Controls.
- Vendors are required to demonstrate compliance with these standards and practices as part of their ongoing engagement.

9. Escalation Procedures:

- Establish escalation procedures for addressing significant vendor cybersecurity issues that may pose a high level of risk to the college.
- Escalation procedures ensure that senior management is informed and can make informed decisions regarding the vendor relationship.

10. Risk Assessment and Risk Mitigation:

- Conduct quarterly monitoring of vendor BitSight scores to assess potential cybersecurity risks associated with their services.
- Apply risk mitigation measures as needed, including enhanced monitoring or additional security controls.

By adhering to these vendor assessment and monitoring procedures, Ramapo College can proactively manage third-party cybersecurity risks and ensure that vendors maintain high standards of cybersecurity. BitSight's continuous monitoring provides valuable insights into vendor security performance, enabling the college to make informed decisions and maintain a secure vendor ecosystem.

XIII. Compliance and Regulations:

Ensuring Compliance with Cybersecurity Laws and Regulations:

Ramapo College is committed to complying with relevant cybersecurity laws and regulations to protect sensitive data and maintain the privacy and security of its stakeholders. Compliance with laws such as the Payment Card Industry Data Security Standard (PCI DSS), the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the Gramm-Leach-Bliley Act (GLBA) is paramount. Here's how the college ensures and maintains compliance:

1. Regulatory Assessment and Alignment:

- Annually assess the college's cybersecurity policies, procedures, and practices to ensure alignment with applicable laws and regulations, including FERPA, HIPAA, NIST 800-171, PCI DSS, and GLBA.
- Identify areas where compliance improvements are needed and establish a plan to address deficiencies.

2. Data Classification and Handling:

- Classify all data within the college's environment based on sensitivity and regulatory requirements.
- Implement data handling procedures that align with the specific regulations governing data protection and privacy.
- Ensure that handling is in line with the Policy 410: Data Protection (PII).

3. Compliance Officer:

- Appoint a designated Compliance Officer/Internal Auditor responsible for overseeing and ensuring compliance with relevant cybersecurity laws and regulations.
- The Compliance Officer/Internal Auditor stays informed about changes in regulations and communicates updates to relevant stakeholders.

4. Regular Training and Awareness:

- Provide regular training and awareness programs for employees and stakeholders to educate them about their roles and responsibilities in maintaining compliance.
- Ensure that training materials are updated to reflect changes in regulations.

5. Risk Assessments:

- Conduct periodic risk assessments to identify and evaluate cybersecurity risks associated with compliance obligations.
- Develop risk mitigation strategies and prioritize actions based on risk levels.

6. Vendor Management:

- Enforce contractual obligations with third-party vendors to ensure they also comply with relevant regulations when handling college data.
- Include vendor compliance assessments as part of the vendor assessment and monitoring procedures.

7. Incident Response:

- Develop and maintain an incident response plan that explicitly addresses incidents related to data breaches, as required by applicable regulations.
- Ensure that the plan includes procedures for notifying affected individuals, regulatory bodies, and law enforcement when necessary.

8. Audit and Assessments:

- Conduct regular compliance assessments and audits to verify adherence to regulations and identify areas for improvement.
- Ensure that audit results are documented and shared with relevant stakeholders.

9. Documentation and Records Management:

- Maintain records of compliance efforts, including risk assessments, training records, audit results, and incident response actions.
- Properly store and manage records to facilitate compliance reporting and audits.

By following these practices, Ramapo College can ensure ongoing compliance with relevant cybersecurity laws and regulations, maintain a proactive approach to cybersecurity, and adapt to changes in the regulatory landscape effectively. Compliance is an ongoing process that requires vigilance, regular review, and a commitment to protecting sensitive data.

XIV. PHYSICAL SECURITY

Addressing Physical Security Measures for Data Centers and Server Rooms: Physical security is a critical aspect of a comprehensive cybersecurity strategy, as it ensures the protection of the physical assets that house and support digital information and systems. To align physical security practices with cybersecurity goals and safeguard data centers and server rooms, Ramapo College implements the following measures:

1. Access Control:

- Stringent access control measures are implemented to restrict physical access to data centers and server rooms. Access is restricted by ID card access.
- An access control list (ACL) that specifies who is authorized to enter these areas is maintained using Millennium. Access control is monitored by the Office of Public Safety.

2. Security Perimeter:

- A secure perimeter around data centers and server rooms, including physical barriers such as fences, walls, or access-controlled doors, is established using a combination of physical locks, security cameras, and ID card access.

3. Surveillance and Monitoring:

- Security cameras and surveillance systems are installed to monitor the physical premises 24/7. These cameras are monitored by the Office of Public Safety.

4. Alarm Systems:

- Install alarm systems that activate in response to unauthorized access, breach attempts, or physical security breaches.
- Ensure that alarms are monitored and responded to promptly.

5. Environmental Controls:

- Environmental controls, such as temperature and humidity monitoring, are maintained to ensure optimal conditions for equipment housed in data centers and server rooms. In addition, fire detection and suppression systems exist to protect against environmental hazards.

6. Redundancy and Backup Power:

- Ensure that data centers and server rooms have backup power supplies, such as uninterruptible power supplies (UPS) or generators, to prevent downtime during power outages.

7. Secure Racks and Cabinets:

- Server racks and cabinets are equipped with locks to prevent unauthorized access to individual servers and network equipment.

8. Personnel Training:

- Personnel responsible for data centers and server rooms are trained annually in security protocols via the IRP tabletop exercises, including physical security measures and emergency response procedures.

9. Integration with Cybersecurity:

- Physical security practices are reviewed annually to align with the broader cybersecurity strategy, focusing on the protection of both physical and digital assets, in collaboration with the Facilities and Public Safety offices. Physical security training is provided through IRP tabletop exercises, which emphasize the need for communication with the Facilities Department and Public Safety when physical security is compromised. The ITS team is trained on when and how to engage with these offices effectively.
- Working together with the cybersecurity team, Facilities, and Public Safety also address security vulnerabilities that affect both physical and digital domains.

By implementing these physical security measures and integrating them with cybersecurity practices, Ramapo College can effectively safeguard its data centers and server rooms against physical threats, ensuring the overall security and availability of critical digital assets. Physical security works hand-in-hand with cybersecurity to create a comprehensive defense strategy.

XV. Business Continuity and Disaster Recovery:

Ramapo College's comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are outlined in the document titled “RCNJ IT Business Continuity Plan.”

XVI. Review and Revision

Establishing a Regular Review Process for the Cybersecurity Policy: To ensure the effectiveness of the CPCM and keep it aligned with emerging threats and evolving technology, Ramapo College follows a regular review and update process. Here's how the process is structured:

1. Review Frequency:

- Conduct a formal review of the CPCM at least annually.
- Additionally, initiate reviews in response to significant security incidents, changes in regulations, or emerging threats.

2. Review Committee:

- The CPCM is initially reviewed and updated by the ITS department, which possesses expert knowledge in cybersecurity. After making necessary changes, the CPCM follows the college’s standard review process:

- Revisions are reviewed and approved by ITS Leadership, in collaboration with the Vice President of Operational & Administrative Integration.
- The CPCM is then submitted to the Policy Review Committee to secure final approval and distribution.
- Internal ITS department policies, relevant solely to the department, may be approved directly by the Chief Information Officer.

3. Assessment Criteria:

- Risk Mitigation Effectiveness: Evaluate the CPCM's success in reducing cybersecurity risks through incident tracking, such as the frequency and severity of security incidents over a defined period.
- Regulatory Compliance: Measure alignment with current and evolving regulatory requirements (e.g., GLBA, FERPA) and ensure the CPCM is updated accordingly.
- Response to Emerging Threats: Assess how the CPCM addresses emerging cybersecurity threats, technologies, and trends (e.g., zero-day vulnerabilities, new attack vectors).
- Stakeholder Feedback: Gather and review feedback from key stakeholders (e.g., ITS, Facilities, Public Safety) on the CPCM's clarity, effectiveness, and areas for improvement.
- Continuous Learning & Improvement: Track the CPCM's adaptability to changes in the threat landscape and its alignment with industry best practices and standards.
- Training and Awareness: Evaluate the effectiveness of training programs and awareness campaigns related to the CPCM, focusing on incident prevention and response preparedness.

4. Emerging Threat Assessment:

- Stay informed about emerging cybersecurity threats and trends through threat intelligence feeds, industry reports, and collaboration with industry peers.
- Assess the relevance of emerging threats to the college's environment and evaluate the CPCM's capacity to address them.

5. Technological Advancements:

- Keep abreast of evolving technologies, including cloud computing, Internet of Things (IoT), and artificial intelligence (AI), and assess their impact on cybersecurity.
- Evaluate whether the CPCM adequately addresses the security implications of new technologies.

6. Incident Analysis:

- Analyze security incidents and breaches that have occurred since the last CPCM review.
- Identify any weaknesses that may have contributed to incidents and determine how these weaknesses can be addressed.

7. Training and Awareness:

- Conduct training sessions and awareness programs to educate employees and stakeholders about the updated CPCM and the reasons for the changes.
- Ensure that all individuals subject to the CPCM are aware of their responsibilities.

8. Testing and Validation:

- Validate the effectiveness of CPCM updates through testing, including vulnerability assessments and security audits, similar to the IRP tabletop exercises.
- Address any identified issues promptly to ensure that Policy and Procedure 411: Cybersecurity and the CPCM achieve intended goals.

14. Ongoing Monitoring:

- Continuously monitor the implementation of the updated CPCM and gather feedback from end-users and IT staff.
- Make adjustments as needed to address any unforeseen challenges or issues.

By following this regular review and update process, Ramapo College can adapt to changing cybersecurity landscapes, respond to emerging threats, and leverage evolving technologies while maintaining a strong and effective cybersecurity policy. The dynamic nature of cybersecurity requires continuous improvement and adaptation to ensure the protection of critical assets and data.

XVII. NON-COMPLIANCE

Defining Consequences for Non-Compliance with the Cybersecurity Policy: Ramapo College recognizes the critical importance of cybersecurity and expects all individuals, including employees, contractors, and stakeholders, to adhere to Policy and Procedure 411: Cybersecurity and the CPCM. Non-compliance with these resources can lead to significant risks and potential harm to the college's digital assets and reputation. To stress the importance of compliance, the college defines consequences for non-compliance, including disciplinary actions for employees:

1. Progressive Disciplinary Actions:

- Ramapo College follows a progressive disciplinary approach for employees who fail to comply with the CPCM, with the flexibility to apply appropriate consequences based on the severity and intent of the violation. Matters will be referred to POER and potential consequences include:

- **Termination**: In cases of severe or intentional violations that jeopardize the college's security or sensitive data, immediate termination may be considered, even for a first offense.
- **Written Warning**: For less severe violations, a written warning may be issued, documenting the breach and outlining the potential consequences of continued non-compliance.
- **Suspension**: For serious or repeated violations, employees may be suspended and required to undergo cybersecurity training and awareness programs before returning to work.

The severity of the violation will guide the disciplinary response, ensuring that the full range of consequences can be applied as needed, regardless of whether the violation is a first-time occurrence.

2. Contractual and Vendor Consequences:

- Contractors, vendors, and other third parties engaged by Ramapo College are contractually obligated to comply with the College's Policy and Procedure 411: Cybersecurity and the CPCM. Non-compliance can lead to:
  - Contract Termination: Breach of cybersecurity requirements may result in the termination of contracts and agreements.
  - Financial Penalties: Non-compliant vendors may incur financial penalties or sanctions as outlined in contracts.
  - Legal Actions: In cases of severe non-compliance or data breaches attributable to third parties, legal actions may be pursued.

3. Loss of Privileges:

- Non-compliance may lead to the loss of access privileges to specific systems, networks, or data.
- Access restrictions will remain in place until individuals complete required cybersecurity training and demonstrate a commitment to compliance.

4. Legal and Regulatory Consequences:

- Non-compliance with cybersecurity regulations and laws may result in legal actions, fines, or penalties against individuals and the college as a whole.

- Ramapo College is committed to upholding its legal obligations and cooperating with relevant authorities.

5. Reporting and Transparency:

- All individuals are required to promptly report (See Section XIX. 7) cybersecurity violations, security incidents, or potential threats.

XVIII. Stressing Everyone's Role in Maintaining Cybersecurity

Ramapo College emphasizes that cybersecurity is a collective responsibility that extends to all individuals, regardless of their roles. Ramapo College stresses the importance of everyone's role in maintaining cybersecurity through the following components and principles:

1. Awareness and Training:

- Cybersecurity training and awareness programs are provided to educate all personnel about their responsibilities and the potential consequences of non-compliance.

2. Employee Accountability:

- All employees have a duty to protect the college's digital assets and data.
- Cybersecurity is not solely the responsibility of IT personnel but is a shared responsibility across the organization.

3. Leadership and Support:

- Senior leadership sets an example by prioritizing and demonstrating commitment to cybersecurity.
- Support and resources are allocated to ensure that all personnel have the tools and knowledge necessary to fulfill their cybersecurity responsibilities.

4. Reporting and Incident Response:

- Employees are educated on how to report security incidents or policy violations.
- Incident response processes are clearly defined and explain how individuals can contribute to their success.

By defining consequences for non-compliance and stressing the importance of everyone's role in maintaining cybersecurity, Ramapo College reinforces a culture of security, accountability, and vigilance, reducing the risk of security breaches and protecting critical digital assets.

XIX. Communication

Ramapo College places great emphasis on the communication, acknowledgment, and ongoing review of Policy and Procedure 411: Cybersecurity and the CPCM to ensure that all employees and stakeholders are aware of their roles and responsibilities in maintaining a secure digital environment. Here's how the college achieves this:

1. Policy Communication:

- The CPCM is made easily accessible and prominently displayed on the college's internal portals.

2. Acknowledgment of Understanding:

- All employees and relevant stakeholders are required to acknowledge their understanding of the Policy and Procedure 411: Cybersecurity, and the CPCM upon hiring.
- Upon hiring or engagement, individuals receive the CPCM, review it, and confirm their understanding and commitment to compliance.

3. Training and Awareness:

- Monthly cybersecurity training and awareness programs have been developed to educate employees and stakeholders about the CPCM's contents, best practices, and evolving threats.
- Training is tailored to different roles and responsibilities within the college.

4. Involvement of Stakeholders:

- Key stakeholders, including IT staff, legal counsel, senior management, and representatives from various departments, are involved in the development, implementation, and review of the CPCM.
- Input and feedback from stakeholders are constantly encouraged to ensure the CPCM aligns with their specific needs and responsibilities.

5. Regular Review and Updates:

- Annual reviews of the CPCM are conducted to evaluate its effectiveness and alignment with emerging threats and technologies.
- The Institutional Policy Committee, composed of representatives from all cores within the college, is engaged to assess the CPCM and recommend updates.
- Updates must address evolving cybersecurity risks and regulations.

6. Incident Response and Learning:

- Lessons learned from security incidents and breaches are integrated into CPCM revisions.
- Real-world incidents are used as case studies in training programs to illustrate the importance of compliance.

7. Clear Reporting Mechanisms:

- Any violations, security incidents, or potential threats related to the CPCM should be promptly reported to the Chief Information Officer (CIO). The CIO will collaborate with ITS Leadership to gather relevant information and recommend appropriate mitigation actions, if applicable. A detailed report will then be generated and, based on the nature of the incident, may be escalated to the Vice President of Operational & Administrative Integration. In certain cases, the incident may also be reported to Legal Counsel, the external cyber insurer, or the Board of Trustees.
- A culture of reporting is encouraged through emphasis on early detection and reporting and how they are crucial to mitigating security risks.

8. Executive Leadership Support:

- Visible and vocal support from senior leadership, including endorsement and promotion of the CPCM, is encouraged.
- Leadership's commitment sets the tone for the entire organization.

9. Legal and Regulatory Compliance:

- The Policy and Procedure 411: Cybersecurity and the CPCM reflect the college's commitment to legal and regulatory compliance, including FERPA, PCI-DSS, HIPAA, NIST CSF, and GLBA.
- The CPCM is reviewed annually and updated to align with changing compliance requirements.

By implementing these practices, Ramapo College establishes a culture of cybersecurity awareness, continuous improvement, and accountability. Effective communication, acknowledgment, and ongoing review of the cybersecurity policy are essential components of a dynamic cybersecurity program that adapts to new threats and technologies while protecting the college's digital assets and reputation.