

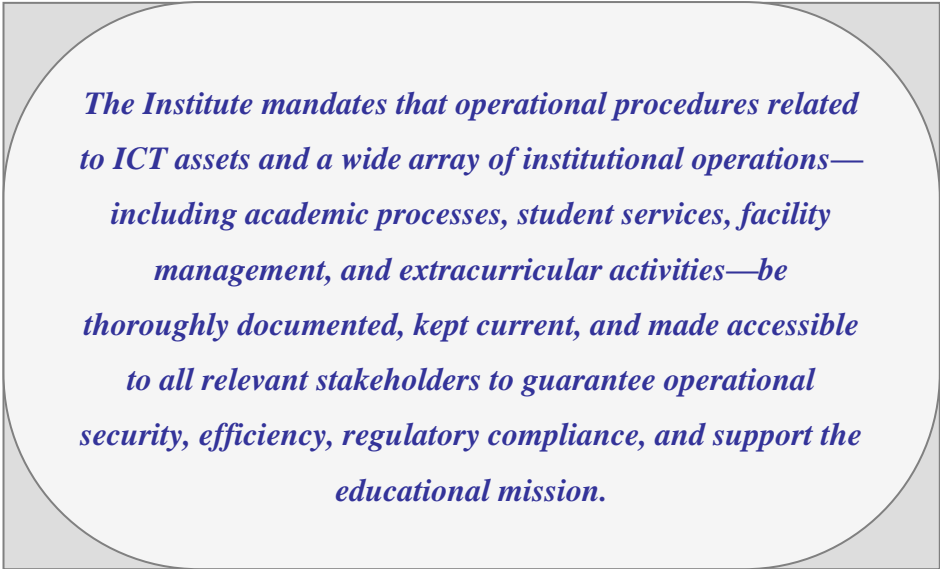
A.12 Operations security

A.12.1 Operational Procedures and Responsibilities

A.12.1.1 Documented Operating Procedures

Objective

To ensure the secure and efficient management of the Institute's Information and Communication Technologies (ICT) assets and institutional operations, safeguarding against unauthorized access, maintaining operational continuity, and ensuring comprehensive documentation across all facets of the Institute's activities.



The Institute mandates that operational procedures related to ICT assets and a wide array of institutional operations—including academic processes, student services, facility management, and extracurricular activities—be thoroughly documented, kept current, and made accessible to all relevant stakeholders to guarantee operational security, efficiency, regulatory compliance, and support the educational mission.

Scope

This policy encompasses all operational aspects of the Institute, extending to faculty, staff, administration, students, interns, partners, and encompasses the management, operation, or use of the Institute's ICT resources, academic regulations, student services, and campus facilities.

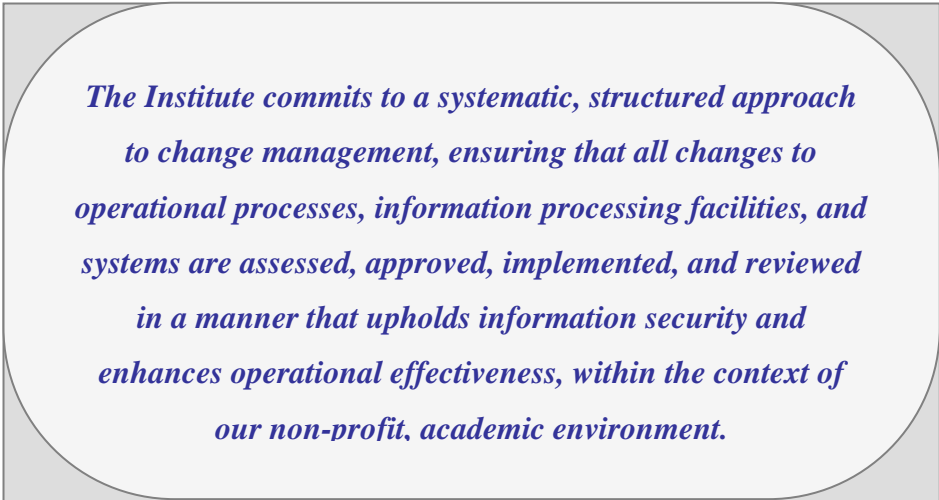
Justification

The need for comprehensive documented procedures is underscored by the complexities of maintaining a secure, compliant, and efficient operational environment within a dynamic educational setting. Documenting procedures across academic and non-academic domains provides a structured approach to risk management, ensures compliance, maintains institutional integrity, facilitates effective collaboration, and underpins quality control across all operations.

A.12.1.2 Change Management

Objective

To establish a controlled framework for managing changes to the organization's operational processes, information processing facilities, and systems that affect information security. This ensures the integrity, availability, and confidentiality of information assets across all operational areas including academic, administrative, and facility management.



The Institute commits to a systematic, structured approach to change management, ensuring that all changes to operational processes, information processing facilities, and systems are assessed, approved, implemented, and reviewed in a manner that upholds information security and enhances operational effectiveness, within the context of our non-profit, academic environment.

Scope

This policy applies to all changes to the Institute's operational processes (including academic, administrative, hostel management, mess management, and canteen operations), information systems, and technological infrastructure that could impact information security. It encompasses changes initiated by faculty, staff, administration, students, interns, and partners.

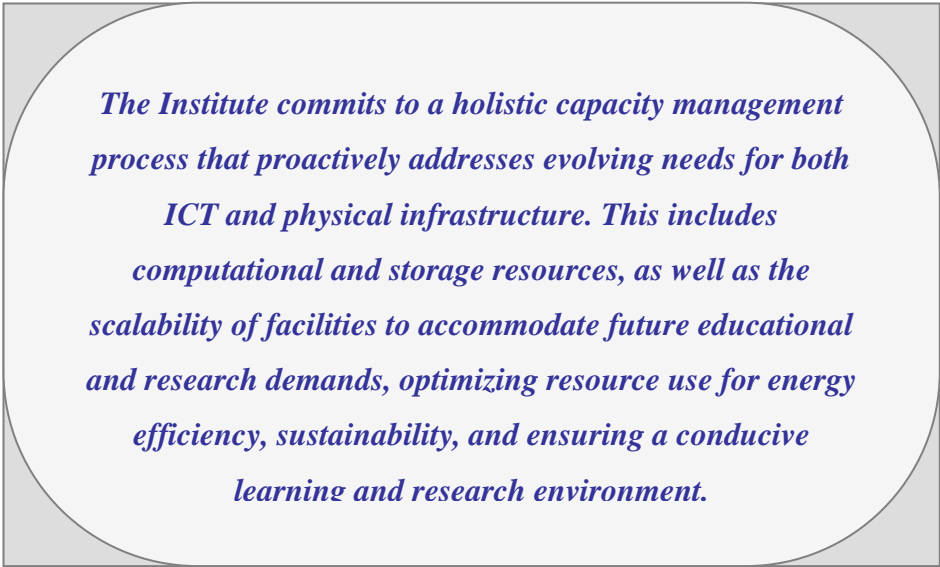
Justification

In a dynamic academic landscape, the importance of a robust change management policy is magnified by the need for adaptability in operational processes, the collaborative nature of academic and research environments, and the necessity to maintain security amid changing cybersecurity threats and compliance requirements. Effective change management ensures the Institute's operational flexibility, supports educational and research excellence, and aligns with the expectations of our academic community and stakeholders.

A.12.1.3 Capacity Management

Objective

To ensure the efficient and effective utilization of the Institute's ICT and physical resources, including computational, storage, networking, messes, hostels, classrooms, halls, and amphitheatres. This involves ongoing monitoring, tuning, and forecasting of capacity requirements to support operational performance, academic activities, resource-intensive research, and comply with regulatory standards without compromising security or operational efficiency.



The Institute commits to a holistic capacity management process that proactively addresses evolving needs for both ICT and physical infrastructure. This includes computational and storage resources, as well as the scalability of facilities to accommodate future educational and research demands, optimizing resource use for energy efficiency, sustainability, and ensuring a conducive learning and research environment.

Scope

This policy applies to all ICT resources (computational, storage, networking) and physical resources (academic and residential facilities) within the Institute. It covers activities related to monitoring current usage, planning for future capacity needs, and managing resource allocation to ensure optimal performance and utilization across all user groups, including faculty, staff, students, and research partners.

Justification


Effective capacity management is essential for supporting the Institute's wide range of activities, from resource-intensive ICT research to academic and residential life, ensuring infrastructure resilience, enabling scalability for innovation, managing cybersecurity demands, promoting energy efficiency, facilitating effective learning and research environments, and ensuring

compliance with regulatory requirements. This policy is designed to support the Institute's strategic objectives by ensuring that both ICT and physical resources are managed efficiently to support high-level research, educational activities, and campus life.

A.12.1.4 Separation of Development, Testing, and Operational Environments

Objective

To ensure the integrity, security, and reliability of the Institute's information systems by enforcing a clear separation between development, testing, and operational environments. This separation aims to minimize the risk of unauthorized access, prevent unintended changes to the operational environment, and ensure the continuity and integrity of core operations.



The Institute is dedicated to sustaining separate environments for development, testing, and operational activities, essential for safeguarding the operational integrity, ensuring data protection compliance, facilitating quality assurance, and optimizing resource use and change management processes.

Scope

This policy applies to all information systems and infrastructure within the Institute, including those used for research, administration, and any collaborative projects. It encompasses all personnel involved in software development, testing, and system administration, including faculty, staff, students, interns, and external partners.

Justification

The separation of environments is essential for fostering innovation and development without compromising the security and functionality of operational systems. It ensures cybersecurity leadership by reducing the risks associated with unauthorized access and changes, supports the secure and compliant handling of data, and enhances quality assurance processes. Moreover, it aids in efficiently managing resources and streamlining change management processes, thus maintaining the Institute's research continuity and protecting intellectual property.

A.12.2 Protection from malware

A.12.2.1 Controls against Malware

Objective

To establish and maintain safeguards against the introduction, effects, and spread of malware across all information processing facilities of the institute, ensuring the integrity, availability, and confidentiality of data.

All information processing facilities must employ up-to-date anti-malware solutions, and regular scans must be conducted to detect and remediate any malware presence.

Scope

This policy applies to all systems, networks, and devices operated by the institute, including those used by employees, faculty, students, contractors, and any other party working in conjunction with the institute.

Justification


Malware poses a critical threat to educational institutions, potentially compromising sensitive research data and personal information. Given the geopolitical complexities and cybersecurity landscape of Tel Aviv, proactive measures are crucial for defense against both opportunistic and targeted cyber threats. Implementing stringent anti-malware controls, combined with user education, forms a dual layer of protection essential for the institute's cybersecurity posture.

A.12.3 Backup

A.12.3.1 Information Backup

Objective

To maintain and restore the integrity and availability of information and information processing facilities by ensuring regular backups are performed and effectively managed.



The institute must establish and follow a comprehensive backup policy, which includes routine backups of all critical information and system images, with regular testing of backup restorations to confirm data integrity and reliability.

Scope

This policy mandates regular backups of all institutional data, software, and system images and is applicable across all departments and units of the institute. This includes data stored on-premises and in cloud services used by the institute.

Justification

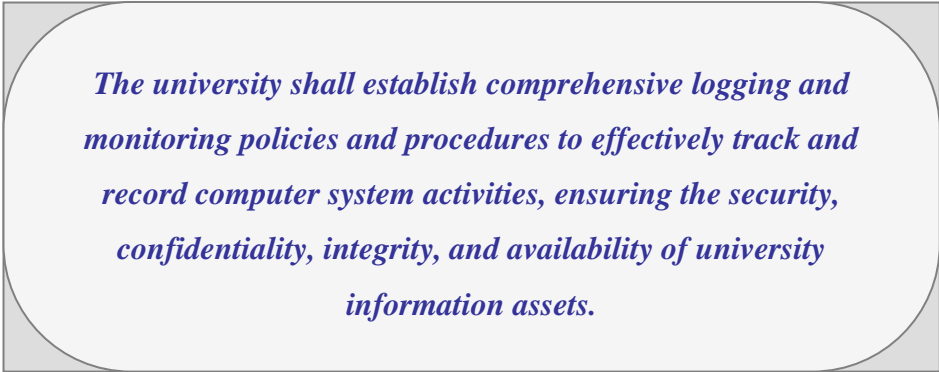
Reliable backup systems are vital for the institute's resilience, given the high stakes of academic data integrity and the need for business continuity. The geopolitical sensitivity of Tel Aviv, alongside risks from cyber-attacks, natural disasters, or technical malfunctions, necessitates a robust backup strategy. This approach ensures that the institute's academic and administrative operations can withstand and quickly recover from disruptive incidents, preserving the educational mission and safeguarding against data loss. Regularly tested backups also contribute to compliance with regulatory requirements and international best practices for information security.

A.12.4 Logging and Monitoring

A.12.4.1 Event logging Policy

Objective

To establish comprehensive logging and monitoring policies and procedures that enable the university to effectively track and record computer system activities, ensuring the security, confidentiality, integrity, and availability of university information assets.



The university shall establish comprehensive logging and monitoring policies and procedures to effectively track and record computer system activities, ensuring the security, confidentiality, integrity, and availability of university information assets.

Scope

Implement logging and monitoring policies across all university-owned computer systems to track user activities, enhance security, ensure compliance with regulations, improve incident response capabilities, promote user awareness, and facilitate continuous improvement.

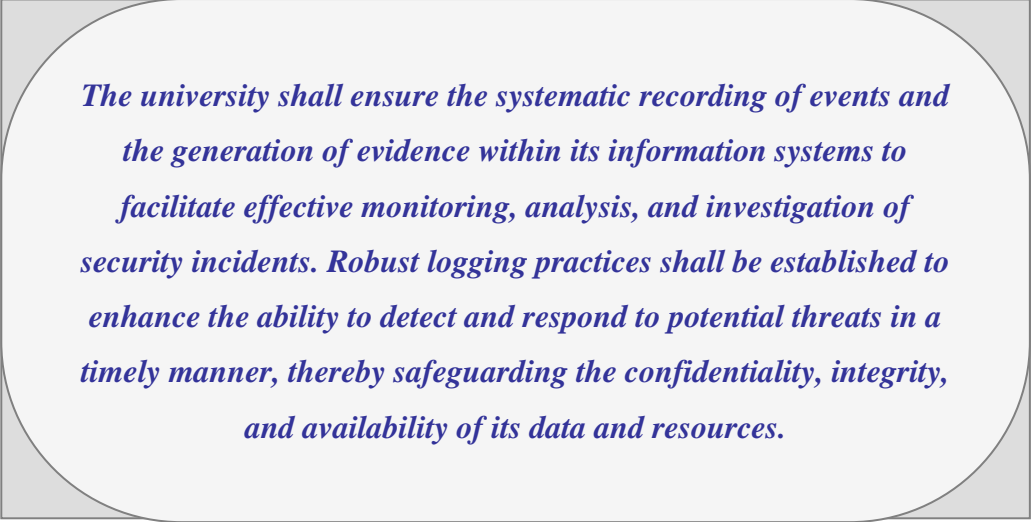
Justification

Implementation of logging and monitoring policies is crucial as it strengthens security measures, aligns with regulatory requirements, reduces risks associated with cybersecurity incidents, enhances incident response readiness, fosters user accountability and awareness, and enables ongoing enhancement of cybersecurity practices within the university.

A.12.4.2 Protection of Log Information

Objective

Implement comprehensive measures to protect log information from tampering and unauthorized access, ensuring the integrity and reliability of logs for security incident monitoring and investigation. This involves implementing access controls, encryption, and integrity checks to prevent unauthorized alterations and preserve evidential value.



The university shall ensure the systematic recording of events and the generation of evidence within its information systems to facilitate effective monitoring, analysis, and investigation of security incidents. Robust logging practices shall be established to enhance the ability to detect and respond to potential threats in a timely manner, thereby safeguarding the confidentiality, integrity, and availability of its data and resources.

Scope

This policy applies to all logging facilities and log information within the college's information systems, including event logs generated by computers, servers, networking equipment, and software applications. It encompasses all staff, faculty, and students who have access to or are responsible for managing logging facilities, ensuring that protection measures are implemented consistently across the organization.

Justification

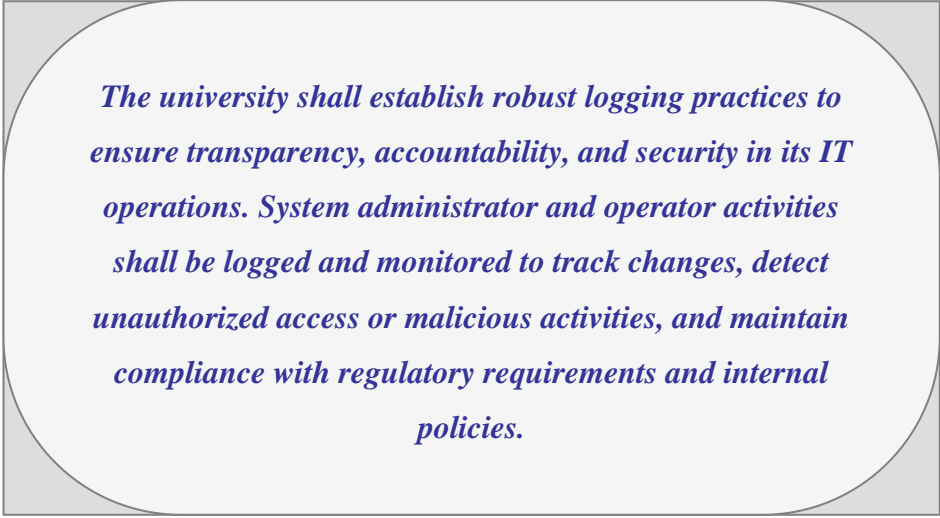
In addition to the points mentioned, securing log information serves several other critical purposes. Firstly, it enhances the organization's incident response capabilities by providing a comprehensive audit trail of system activities, enabling the identification and analysis of security incidents and breaches. Moreover, protecting log data ensures the preservation of evidentiary value, supporting legal and regulatory compliance requirements and facilitating effective resolution of disputes or investigations. Furthermore, robust logging practices can aid in the identification of system weaknesses and vulnerabilities, enabling proactive measures to strengthen the organization's overall security posture. Additionally,

safeguarding log information fosters transparency and accountability within the organization, instilling confidence among stakeholders regarding the integrity of its information systems and the reliability of its security measures. Finally, adherence to logging security controls aligns with industry best practices and standards, demonstrating the college's commitment to maintaining a robust and resilient cybersecurity framework in line with evolving threats and regulatory expectations.

A.12.4.3 Administrator and operator logs Policy

Objective

The objective of this policy is to establish robust logging practices to ensure transparency, accountability, and security in the university's IT operations. By logging and monitoring system administrator and operator activities, the policy aims to track changes, detect unauthorized access or malicious activities, and maintain compliance with regulatory requirements and internal policies.



The university shall establish robust logging practices to ensure transparency, accountability, and security in its IT operations. System administrator and operator activities shall be logged and monitored to track changes, detect unauthorized access or malicious activities, and maintain compliance with regulatory requirements and internal policies.

Scope

This policy applies to all system administrators and operators responsible for managing and maintaining the university's IT infrastructure, including servers, networks, databases, and applications. It encompasses all activities performed by administrators and operators, whether they involve system configurations, user management, software installations, or other administrative tasks. The policy extends to all university-owned devices, systems, and applications, regardless of their physical location or network connectivity.

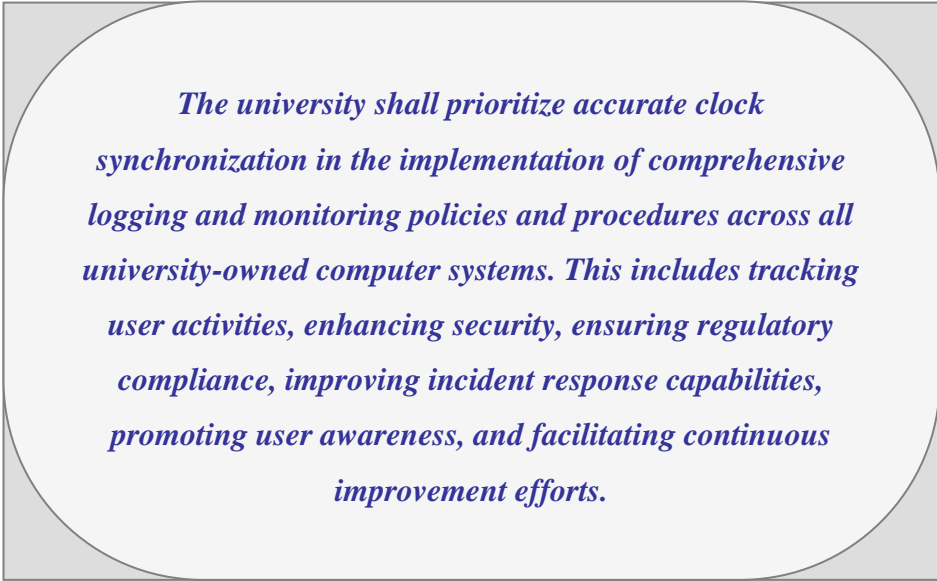
Justification

This policy is essential to ensure transparency and accountability in the university's IT operations. By logging and protecting system administrator and operator activities, the university can track changes made to the system, monitor access by privileged users, and detect any suspicious activities. Regular review of these logs helps identify unauthorized actions and ensures compliance with policies and regulations, thereby enhancing the overall security posture of the university's IT infrastructure.

A.12.4.4 Clock synchronization

Objective

Establish comprehensive logging and monitoring policies and procedures, prioritizing accurate clock synchronization to effectively track and record computer system activities. This ensures the security, confidentiality, integrity, and availability of university information assets by enabling precise timeline correlation during incident investigations and audits.



The university shall prioritize accurate clock synchronization in the implementation of comprehensive logging and monitoring policies and procedures across all university-owned computer systems. This includes tracking user activities, enhancing security, ensuring regulatory compliance, improving incident response capabilities, promoting user awareness, and facilitating continuous improvement efforts.

Scope

Implement logging and monitoring policies across all university-owned computer systems, emphasizing accurate clock synchronization. This enables precise event sequencing, enhances security, ensures regulatory compliance, bolsters incident response capabilities, fosters user awareness, and supports continuous improvement efforts.

Justification

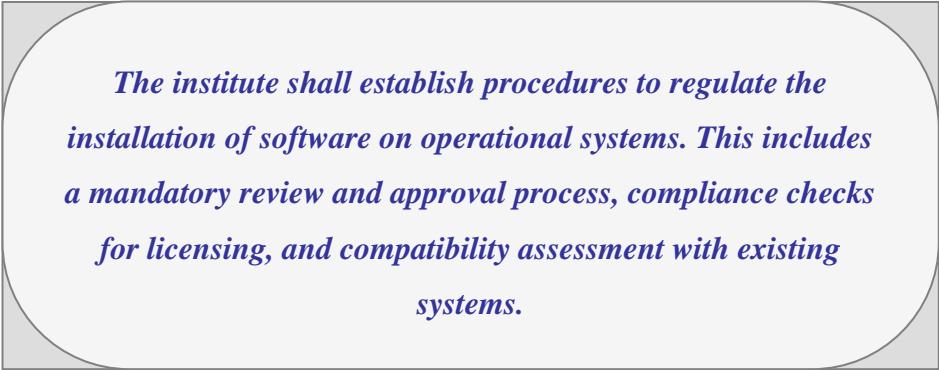
Accurate clock synchronization is crucial for maintaining the integrity and reliability of logs, enabling precise timeline reconstruction during incident investigations and audits. It aligns with regulatory requirements, reduces risks associated with cybersecurity incidents, enhances incident response readiness, promotes user accountability and awareness, and facilitates ongoing enhancement of cybersecurity practices within the university.

A.12.5 Control of Application Software

A.12.5.1 Installation of Software on Operational System

Objective

To preserve the integrity and stability of the institute's operational systems by ensuring that software installations are managed and controlled.



The institute shall establish procedures to regulate the installation of software on operational systems. This includes a mandatory review and approval process, compliance checks for licensing, and compatibility assessment with existing systems.

Scope

This policy applies to all systems, networks, and devices operated by the institute, encompassing those utilized by employees, faculty, students, contractors, and any external parties engaged with the institute's technological resources.

Justification

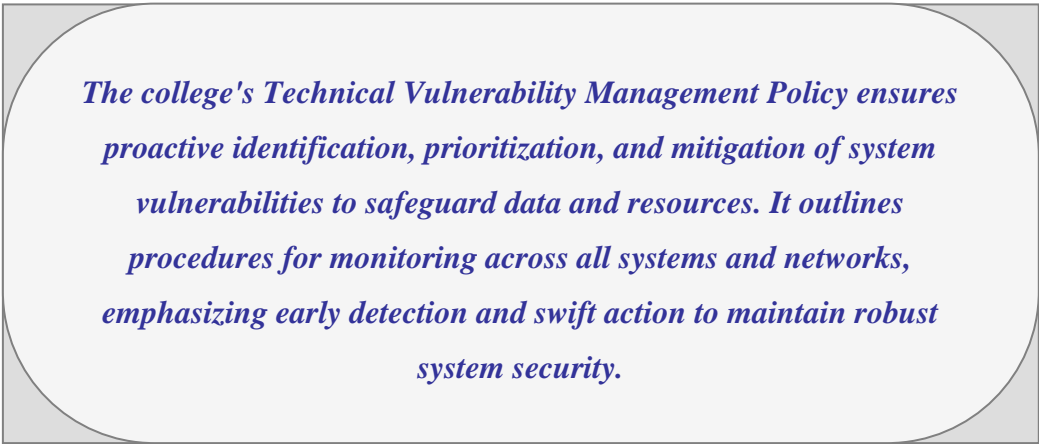
Effective control over software installations is critical to prevent security vulnerabilities, system conflicts, and resource inefficiencies. Given the technological reliance of an educational institute and the increased cyber threats in a geopolitically complex city like Tel Aviv, such controls are essential to safeguard operational systems. This policy not only supports the institute's security posture but also upholds legal compliance and operational consistency, which are indispensable for maintaining the institute's reputation for academic excellence and operational integrity.

12.6 Technical vulnerability management Policy

12.6.1 Management of Technical Vulnerabilities

Objective

To prevent the exploitation of technical vulnerabilities within the college's information systems, safeguarding the confidentiality, integrity, and availability of data and resources. This objective underscores the importance of proactively identifying and addressing vulnerabilities to mitigate the risk of cyberattacks and unauthorized access to sensitive information.



The college's Technical Vulnerability Management Policy ensures proactive identification, prioritization, and mitigation of system vulnerabilities to safeguard data and resources. It outlines procedures for monitoring across all systems and networks, emphasizing early detection and swift action to maintain robust system security.

Scope

This policy applies to all information systems, networks, and devices owned or operated by the college, ensuring comprehensive coverage of cybersecurity measures. It includes computers, servers, networking equipment, and software applications utilized in academic, administrative, and research activities, emphasizing the need for a holistic approach to vulnerability management.

Justification

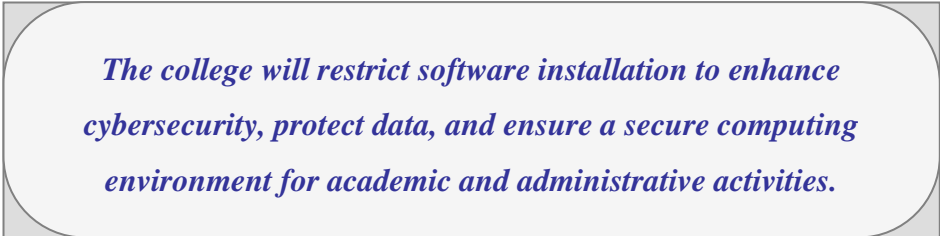
In today's rapidly evolving cybersecurity landscape, it's imperative to maintain robust vulnerability management practices to mitigate risks effectively. Ensuring the confidentiality and integrity of sensitive data is paramount for compliance with privacy regulations and to uphold trust among stakeholders. Additionally, uninterrupted access to information systems is essential for the smooth functioning of academic and administrative operations. Adhering to

regulatory standards mandates proactive vulnerability management to avoid penalties and safeguard the college's reputation.

12.6.2 Restrictions on software installation

Objective

The objective of this policy is to proactively prevent the exploitation of technical vulnerabilities within the college's information systems by implementing restrictions on software installation. By doing so, the college aims to bolster its cybersecurity defenses and safeguard sensitive data from potential breaches or unauthorized access. Additionally, the policy seeks to promote a secure computing environment conducive to academic and administrative activities, fostering trust among stakeholders and ensuring the continuity of critical operations.



The college will restrict software installation to enhance cybersecurity, protect data, and ensure a secure computing environment for academic and administrative activities.

Scope

This policy applies to all users accessing the college's information systems, including staff, faculty, and students, and extends to all devices connected to the college's network. This includes computers, laptops, servers, and mobile devices, regardless of ownership or location. The policy ensures that all software installations adhere to predefined rules and guidelines established by the college's IT department, promoting consistency and coherence in software management practices.

Justification

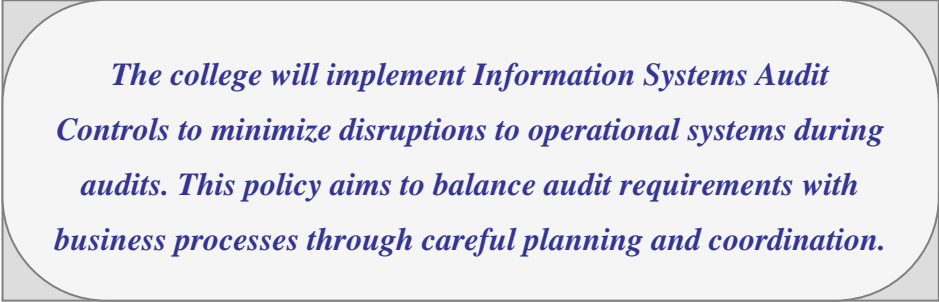
Implementing rules on software installation enhances the overall security posture of the college's information systems by reducing the risk of unauthorized or harmful software installation. It protects valuable information assets from exploitation, minimizes the potential for data breaches, and ensures compliance with regulatory requirements and institutional policies. Furthermore, controlled software installations contribute to the stability and reliability of information systems, empower users to make informed decisions, and enhance operational efficiency by promoting a standardized computing environment. This, in turn, supports the college's strategic objectives of innovation, collaboration, and academic excellence.

12.7 Information systems audit considerations

12.7.1 1 Information systems audit controls

Objective

The objective of this policy is to minimize the impact of audit activities on operational systems within the college's information systems infrastructure. By carefully planning and coordinating audit activities, the college aims to mitigate disruptions to business processes, ensuring the smooth functioning of essential operations while fulfilling audit requirements.



The college will implement Information Systems Audit Controls to minimize disruptions to operational systems during audits. This policy aims to balance audit requirements with business processes through careful planning and coordination.

Scope

This policy applies to all audit requirements and activities conducted within the college's information systems infrastructure in Tel Aviv, Israel. It encompasses audits involving verification of operational systems, including but not limited to, IT systems, networks, and applications. The policy covers all stakeholders involved in audit activities, including audit teams, IT personnel, department heads, and other relevant parties.

Justification

This policy is crucial for balancing audit requirements with operational efficiency. It aims to prevent disruptions caused by audits, ensuring smooth business processes while meeting compliance needs. By adhering to ISO standards, the college demonstrates its commitment to robust information security practices and regulatory compliance, ultimately safeguarding its reputation and operational integrity.

12.1 Operational Procedures and Responsibilities

12.1.1 Documented Operating Procedures

In order to implement the Documented Operating Procedures Policy, the following procedures shall be implemented. The **Documentation and Compliance Oversight Committee**, under the leadership of the **Chief Information Officer (CIO) and the Chief Administrative Officer (CAO)**, is responsible for ensuring the implementation of these procedures.

PROCEDURES

12.1.1.1 Documentation and Oversight

12.1.1.1.1 Broadened Documentation Scope:

- Extend documentation to include rules and regulations governing hostels, academic policies, credit points and assessment criteria, attendance tracking, course selection processes, details of all courses offered, sports and club activities, and comprehensive college infrastructure guidelines.
- Procedures related to student identification, verification processes, and management of personal identification data must be documented and maintained with utmost security.

12.1.1.1.2 Annual Review and Updates:

- Conduct annual reviews or as needed based on significant changes in institutional operations, regulatory updates, or technological advancements, ensuring all documentation is current and reflective of best practices.

12.1.1.2 Access and knowledge Sharing

12.1.1.2.1 Enhanced Access and Distribution:

- Ensure that access to documented procedures is controlled yet sufficiently accessible through a secure digital repository, catering to the specific needs of various stakeholders within the Institute.

12.1.1.2.2 Expanded Training and Awareness:

- Implement comprehensive training programs that include orientations for new members and ongoing training for existing members of the Institute, covering all documented procedures to ensure widespread awareness and compliance.

12.1.1.3 Compliance, Monitoring, and Improvement

12.1.1.3.1 Comprehensive Compliance Audits:

- Perform regular audits across all documented operational areas to verify adherence, with findings addressed proactively by designated institutional managers.

12.1.1.3.2 Continuous Monitoring and Feedback Mechanism:

- Establish continuous monitoring to promptly identify and correct deviations from established procedures. Foster a culture of feedback to continuously refine and enhance operational processes.

12.1.1.4 Incident Management and Innovation

12.1.1.4.1 Inclusive Incident Response:

- Document and maintain a comprehensive incident response plan covering a wide range of potential scenarios, including security breaches, operational failures, and emergency situations across all institutional operations.

12.1.1.4.2 Drills, Simulations, and Feedback:

- Regularly conduct drills and simulation exercises to test the robustness of the incident response plan, incorporating feedback to drive continuous improvement.

12.1.1.5 Knowledge Management and Institutional Growth

12.1.1.5.1 Institutional Knowledge Sharing:

- Develop a knowledge management system that encompasses not only ICT operations but also academic and campus life, facilitating sharing and management of operational knowledge, best practices, and innovations.

12.1.1.5.2 Stakeholder Engagement and Feedback:

- Implement mechanisms for collecting and incorporating feedback on operational procedures from all institutional stakeholders, encouraging a collaborative approach to continuous improvement and innovation.

12.1.2 Change Management

In order to implement the Change Management Policy, the following procedures shall be implemented. The **Change Management Committee**, chaired by the **Chief Operations Officer (COO)** and **co-chaired by the Director of Information Security**, is responsible for ensuring the implementation of these procedures.

PROCEDURES

12.1.2.1 Change Identification and Recording

12.1.2.1.1 Initiation:

- All proposed changes to operational processes or IT systems, regardless of scale, must be formally documented, including a clear description, rationale, security impact assessment, and proposed implementation plan.
- Proposals for change can originate from any member of the Institute's community but must be formally submitted to the Change Management Committee for initial review.

12.1.2.1.2 Documentation:

- A Change Register will be maintained to comprehensively log all proposed, in-process, and completed changes, detailing the assessment, approval, implementation, and post-implementation outcomes.

12.1.2.2 Change Assessment and Approval

12.1.2.2.1 Impact Assessment:

- The Change Management Committee conducts a detailed assessment of each proposed change, evaluating potential effects on information security, operational continuity, and compliance with academic and administrative standards.

12.1.2.2.2 Approval Process:

- Significant or potentially high-impact changes require approval from senior management. More routine modifications may be authorized at the departmental or faculty level, following established guidelines.

12.1.2.3 Change Implementation and Monitoring

12.1.2.3.1 Implementation Planning:

- Each approved change must be supported by a comprehensive implementation plan, outlining schedules, assigned responsibilities, resource allocation, and contingency measures for potential rollback.

12.1.2.3.2 Monitoring and Reporting:

- The implementation phase is subject to close monitoring, with regular progress reports submitted to the Change Management Committee. Deviations from the planned process are addressed promptly.

12.1.2.4 Post-Implementation Review and Feedback

12.1.2.4.1 Review and Analysis:

- A thorough review is conducted following the implementation of each change to evaluate its effectiveness, gather insights, and assimilate feedback for the continual refinement of the change management process.

12.1.2.4.2 Continuous Improvement:

- Feedback and lessons learned are integral to the iterative improvement of the Institute's change management practices, enhancing our ability to respond to new opportunities and challenges.

12.1.2.5 Communication and Training

12.1.2.5.1 Stakeholder Communication:

- Transparent communication ensures all stakeholders are informed about pending changes, their expected impacts, and any necessary preparatory actions.

12.1.2.5.2 Training and Awareness:

- Targeted training and awareness sessions are provided to equip all individuals directly involved in or affected by changes with the knowledge and tools needed to navigate new processes or systems effectively.

12.1.3 Capacity Management

In order to implement the Capacity Management Policy, the following procedures shall be implemented. The **Capacity Management Working Group**, led by the **Director of IT Infrastructure and the Director of Campus Facilities**, is responsible for ensuring the implementation of these procedures.

PROCEDURES

12.1.3.1 Resource Monitoring and Analysis

12.1.3.1.1 Continuous Monitoring:

- Implement tools and processes for real-time monitoring of both ICT systems and physical facility usage to identify trends, peaks, and bottlenecks in resource utilization.
- Regularly review resource utilization against performance benchmarks and capacity requirements to ensure optimal operation across all facilities.

12.1.3.1.2 Performance Analysis:

- Analyse performance data to identify inefficiencies and opportunities for optimization in both ICT and physical infrastructures, including underutilized resources and areas requiring capacity enhancement.

12.1.3.2 Capacity Planning and Forecasting

12.1.3.2.1 Future Needs Projection:

- Utilize predictive analytics to forecast future capacity requirements based on trends, research project pipelines, academic calendar events, and planned technological or infrastructural advancements.
- Prepare and update a comprehensive capacity expansion plan that aligns with the Institute's strategic research objectives, academic needs, and campus life enhancements.

12.1.3.2.2 Scalability and Flexibility:

- Ensure that infrastructure design and procurement strategies for both ICT and physical facilities support scalability and flexibility to accommodate future needs, emerging technologies, and fluctuating academic activities.

12.1.3.3 Resource Optimization and Sustainability

12.1.3.3.1 Optimization Initiatives:

- Undertake resource optimization initiatives to enhance system performance and energy efficiency, including server virtualization, cloud resource integration, and green IT practices, alongside optimizing the use and energy efficiency of physical facilities.
- Implement demand management strategies to align resource allocation with varying workload requirements efficiently, including timetabling for academic facilities to maximize utilization.

12.1.3.3.2 Sustainability Practices:

- Incorporate sustainability practices in capacity planning for both ICT and physical resources, focusing on energy-efficient technologies and reducing the carbon footprint of the Institute's operations.

12.1.3.4 Compliance and Security

12.1.3.4.1 Regulatory Compliance:

- Align capacity management activities with legal and regulatory requirements related to data handling, privacy, security, and facility safety standards.
- Ensure sufficient capacity to support data protection measures and safety protocols in physical facilities, including emergency response capabilities.

12.1.3.4.2 Security Considerations:

- Incorporate security considerations into capacity planning for ICT resources and physical facilities to ensure expansions or modifications do not introduce vulnerabilities.
- Ensure capacity for security tools and systems to handle increasing volumes of security data and analytics, along with physical security measures for campus safety.

12.1.3.5 Collaboration and Communication

12.1.3.5.1 Stakeholder Engagement:

- Engage with key stakeholders, including research departments, academic faculties, student representatives, and IT teams, to understand capacity needs and priorities for both ICT and physical facilities.
- Communicate capacity planning and management policies and procedures to all relevant parties, ensuring clear understanding and compliance.

12.1.3.5.2 Feedback and Adjustment:

- Establish mechanisms for receiving feedback on capacity management and performance issues for both ICT and physical resources.
- Regularly review and adjust capacity management processes based on feedback, technological advances, academic requirements, and changes in campus life needs.

12.1.4 Separation of Development, Testing, and Operational Environments

In order to implement the Separation of Development, Testing, and Operational Environments Policy, the following procedures shall be implemented. The **IT Security and Compliance Unit**, supervised by the **Chief Technology Officer (CTO) and the Information Security Manager (ISM)**, is responsible for ensuring the implementation of these procedures.

PROCEDURES

12.1.4.1 Environment Definition and Segregation

12.1.4.1.1 Establishment of Environments:

- Define and establish clear boundaries between development, testing, and operational environments, with specific protocols for access, data handling, and system configurations.

12.1.4.1.2 Access Control:

- Implement strict access control measures for each environment, ensuring that only authorized personnel have access based on their roles and requirements.

12.1.4.2 Data Management and Protection

12.1.4.2.1 Data Handling Procedures:

- Establish and enforce data handling procedures for each environment, ensuring that production data is anonymised or pseudonymized before use in development or testing environments.

12.1.4.2.2 Compliance Checks:

- Regularly review and audit data management practices in each environment to ensure compliance with data protection laws and policies.

12.1.4.3 Quality Assurance and Testing

12.1.4.3.1 Testing Protocols:

- Develop and implement standardized testing protocols for the testing environment, ensuring that changes are thoroughly vetted before being deployed to the operational environment.

12.1.4.3.2 Error Containment:

- Ensure that errors identified in development or testing phases are contained and resolved without impacting the operational environment.

12.1.4.4 Resource Allocation

12.1.4.4.1 Resource Optimization:

- Allocate resources to each environment based on specific needs and usage patterns to optimize performance and efficiency while maintaining the separation.

12.1.4.4.2 Environment-Specific Tools and Services:

- Utilize environment-specific tools and services that support the unique requirements of development, testing, and operational phases.

12.1.4.5 Change Management Integration

12.1.4.5.1 Change Control Procedures:

- Integrate environment separation principles into the Institute's change management procedures, ensuring that changes are properly developed, tested, and approved before implementation in the operational environment.

12.1.4.5.2 Transition and Deployment Processes:

- Establish clear processes for the transition of tested changes from the development and testing environments to the operational environment, ensuring minimal disruption and maintaining system integrity.

12.2 Malware Protection Policy

12.2.1 Controls against Malware

To enact the Malware Protection Policy, The institute will integrate advanced technological defenses including firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS), alongside rigorous user training to prevent, detect, and respond to malware threats. The Information Security Manager will oversee the deployment and effectiveness of these measures, ensuring comprehensive protection of the institute's information assets.

PROCEDURES

12.2.1.1 Malware Detection and Prevention

- Enterprise-grade antivirus and anti-malware solutions will be installed on all endpoints and servers, with automatic updates for continual protection against new threats.
- All inbound and outbound email traffic, as well as downloads, will be scanned for malware. Detected threats will be isolated and addressed immediately.

12.2.1.2 Network Security Infrastructure

- Firewalls will be deployed at all network perimeters to control access based on security policies.
- Network-based IDS will monitor for unusual activity signaling potential security breaches.
- IPS devices will actively analyze and block detected network threats in real time.

12.2.1.3 System Security Maintenance

- Regular updates and patches for firewalls, IDS, and IPS will be applied within a defined timeframe after release.
- Routine audits and system checks will be conducted to ensure the optimal operation of security systems.

12.2.1.4 User Education and Training

- Periodic and mandatory cybersecurity training sessions will be held for all institute members, focusing on malware risks and the importance of network security infrastructure.
- Users will be trained to recognize the signs of malware and the correct protocol for reporting security incidents to the IT support team.

12.2.1.5 Incident Response and Recovery

- A detailed Incident Response Plan (IRP) will outline the steps for addressing malware infections, from containment to recovery, with an emphasis on minimizing data loss and system downtime.
- Data backups will be performed regularly to ensure the integrity and availability of critical information.

12.2.1.6 Policy Review and Continuous Improvement

- This policy will undergo regular reviews at least annually, or more frequently if significant changes in the threat landscape or technology occur.
- The Information Security Committee will be responsible for reviewing and approving updates or amendments to this policy and related procedures.

12.2.1.7 Compliance

- Adherence to this policy is compulsory for all users, and violations will result in disciplinary action, which may include termination of employment or academic standing.

12.3 Information Backup Policy

12.3.1 Information Backup

To execute the Information Backup Policy, the institute will establish a systematic and verifiable backup routine, ensuring the resilience and recoverability of critical information, software, and system images. The Information Security Manager will supervise the entire backup lifecycle, from creation and maintenance to secure storage and periodic testing, guaranteeing the preservation of data integrity and availability across all operational spectrums of the institute.

PROCEDURES

12.3.1.1 Backup Creation and Management

- Routine backups of all identified critical information shall be executed in accordance with the established backup schedule that reflects the importance and sensitivity of the data.
- The backup process will align with the institute's strategic objectives and comply with relevant data protection and privacy regulations.

12.3.1.2 Backup Testing and Restoration

- All backups will undergo routine testing to confirm data integrity and the effectiveness of the recovery process.
- Documented recovery procedures shall be established, maintained, and readily available to authorized personnel to ensure a swift and secure data restoration capability.

12.3.1.3 Storage and Security of Backups

- Backup media shall be stored securely, with a clear segregation from the primary data. Offsite storage locations will be utilized where appropriate, with stringent access controls and environmental protection.
- Encryption and access controls shall be applied to backup data to ensure its security during both storage and transit.

12.3.1.4 Roles and Responsibilities

- The Information Security Manager shall oversee the implementation and adherence to the backup policy, coordinating with relevant departments for execution and compliance.
- Regular audits will be conducted to ensure compliance with the backup procedures, and findings will be reported to the Information Security Committee.

12.3.1.5 Review and Updates

- The backup policy will be reviewed annually or following significant events to maintain its relevance and effectiveness in line with the evolving data landscape.

- Amendments to the policy will be made under the authority of the Information Security Committee, ensuring the institute's backup strategies adhere to best practices and regulatory requirements.

A.12.4 Logging and Monitoring

12.4.1 Event logging Policy

PROCEDURES

12.4.1.1 Event Logging:

- The institute shall maintain a centralized logging mechanism to record user activities, exceptions, faults, and information security events across all systems and applications.
- Logs shall be generated in a standardized format to facilitate easy review and analysis.

12.4.1.2 Log Retention:

- Logs shall be retained for a minimum period of [specify duration] to facilitate investigation and audit purposes.
- Retained logs shall be protected from unauthorized access, tampering, or deletion.

12.4.1.3 Log Review:

- Logs shall be regularly reviewed by designated personnel to identify and respond to security incidents, anomalies, and potential risks.
- The review process shall include analysis of log entries to detect unauthorized access attempts, unusual user behavior, and system errors.

12.4.1.4 Logging Configuration:

- Logging shall be enabled by default on all systems and applications, with appropriate log levels configured to capture relevant information.
- Configuration changes to logging settings shall be documented and approved by authorized personnel.

12.4.1.5 Incident Response:

- Logs shall be used as part of the incident response process to investigate and mitigate security incidents promptly.
- Incident response procedures shall include the analysis of logs to determine the scope and impact of an incident.

12.4.1.6 Training and Awareness:

- Personnel responsible for managing logs and reviewing log data shall receive training on the importance of event logging and log analysis techniques.
- Awareness campaigns shall be conducted to educate all users about the role of event logging in maintaining information security.

12.4.2 Protection of Log Information

PROCEDURES

12.4.2.1 Logging Facilities Protection:

- Logging facilities, including log servers and storage systems, shall be protected against unauthorized access and tampering.
- Access to logging facilities shall be restricted to authorized personnel only, and access controls shall be implemented to prevent unauthorized changes to logging configurations.

12.4.2.2 Log Information Protection:

- Log information shall be stored securely to prevent unauthorized access, modification, or deletion.
- Logs shall be encrypted both at rest and in transit to protect the confidentiality and integrity of log information.

12.4.2.3 Access Control:

- Access to log information shall be restricted based on the principle of least privilege, with access granted only to authorized personnel for specific purposes.
- Access controls shall be regularly reviewed and updated to ensure they are effective in protecting log information.

12.4.2.4 Monitoring and Alerting:

- Monitoring mechanisms shall be implemented to detect and alert on unauthorized access attempts or tampering with logging facilities or log information.
- Alerts shall be promptly investigated and responded to by designated personnel to mitigate potential security incidents.

12.4.2.5 Audit and Compliance:

- Regular audits shall be conducted to ensure compliance with logging facility protection policies and procedures.
- Audit logs of access to log information and logging facilities shall be maintained and reviewed to detect and respond to potential security incidents.

12.4.3 Administrator and operator logs Policy

12.4.3.1 Administrator and Operator Activity Logging:

- System administrator and system operator activities shall be logged to ensure accountability and traceability.
- Logs shall include details such as user actions, commands executed, and system changes made by administrators and operators.

12.4.3.2 Log Protection:

- Logs of system administrator and system operator activities shall be protected against unauthorized access, modification, or deletion.
- Access to logs shall be restricted to authorized personnel only, and access controls shall be regularly reviewed and updated.

12.4.3.3 Regular Log Review:

- Logs of system administrator and system operator activities shall be regularly reviewed by designated personnel to detect and respond to security incidents or policy violations.
- Reviews shall be conducted at least [specify frequency] to ensure logs are being properly maintained and monitored.

12.4.3.4 Incident Response:

- Logs of system administrator and system operator activities shall be used as part of the incident response process to investigate and mitigate security incidents.
- Incident response procedures shall include the analysis of logs to determine the root cause and impact of an incident.

12.4.3.5 Training and Awareness:

- System administrators and system operators shall receive training on the importance of logging their activities and the proper procedures for accessing and reviewing logs.
- Awareness campaigns shall be conducted to educate all users about the role of logging in maintaining information security.

12.4.4 Clock synchronization

12.4.4.1 Clock Synchronization:

- The clocks of all relevant information processing systems within the institute shall be synchronized to a single reference time source.
- The reference time source shall be a reliable time server, either internal or external, that provides accurate timekeeping.

12.4.4.2 Synchronization Mechanism:

- Synchronization of clocks shall be achieved using a reliable time synchronization protocol, such as Network Time Protocol (NTP) or Precision Time Protocol (PTP).
- All systems shall be configured to synchronize their clocks periodically with the reference time source.

12.4.4.3 Monitoring and Compliance:

- The synchronization status of clocks shall be monitored regularly to ensure compliance with the synchronization policy.
- Any deviations from the synchronization policy shall be promptly investigated and remediated.

12.4.4.4 Backup Time Source:

- A backup time source shall be identified and configured in case the primary reference time source becomes unavailable.
- Systems shall be configured to automatically switch to the backup time source if the primary source is not reachable.

12.4.4.5 Documentation and Auditing:

- Documentation shall be maintained detailing the synchronization configuration of all systems and the reference time source used.
- Regular audits shall be conducted to verify that all systems are synchronized to the reference time source according to the institute's policy.

12.5 Installation of Software on Operational Systems Policy

12.5.1 Installation of software on operational systems

The policy for controlling software installations on operational systems is established to preserve the integrity and stability of institute's technological environment. By instituting a formal approval process for all software installations, the institute ensures operational consistency, adherence to licensing agreements, and protection against unauthorized or harmful software. The Information Security Manager will oversee this process, coordinating with IT staff to maintain system integrity, security, and compliance with this policy.

PROCEDURES

12.5.1.1 Software Installation Control

- A formal process will be established for the request, review, and approval of all software installations on operational systems.
- Only authorized personnel will perform software installations, following a verified and recorded process.
- All software to be installed must have a valid license and be reviewed for compatibility and security before approval.
- A registry of all approved software installations will be maintained along with the respective licenses and version details.

12.5.1.2 Monitoring and Maintenance

- Regular audits will be conducted to ensure compliance with the software installation policy and to detect any unauthorized software.
- Procedures for the timely update of operational software will be established, ensuring that all software remains current and supported.

12.5.1.3 Review and Update

- This policy shall be reviewed annually or in response to significant changes in operational requirements or IT infrastructure to ensure ongoing relevance and efficacy.

12.5.1.5.1 Compliance and Enforcement

- Non-compliance with these procedures may result in disciplinary action. Training will be provided to relevant staff on the importance of this policy and their respective roles and responsibilities.

12.6 Technical vulnerability management

12.6.1 Management of technical vulnerabilities

To enact the Management of Technical Vulnerabilities Policy, the following procedures shall be established. The Vulnerability Management Oversight Committee, led by the Chief Information Officer (CIO) and the Chief Administrative Officer (CAO), is tasked with ensuring the execution of these procedures.

PROCEDURES

12.6.1.1 Guidelines

12.6.1.1.1 Vulnerability Management Policy:

- The college shall establish procedures to identify, assess, and prioritize technical vulnerabilities in its information systems promptly.

12.6.1.1.2 Vulnerability Assessment Procedure:

- Regular assessments shall be conducted to evaluate the organization's exposure to technical vulnerabilities, ensuring timely detection and mitigation.

12.6.1.1.3 Risk Evaluation and Treatment Policy:

- The college shall assess the risks associated with identified vulnerabilities and implement appropriate measures to mitigate these risks effectively.

12.6.1.1.4 Patch Management Policy:

- Procedures shall be established to ensure the timely deployment of patches and updates to address known vulnerabilities in the information systems.

12.6.1.1.5 Vulnerability Response Plan:

- A response plan shall be developed to outline the actions to be taken in the event of a critical technical vulnerability being identified.

12.6.1.1.6 Monitoring and Review Protocol:

- Ongoing monitoring of information systems shall be conducted to detect and address new vulnerabilities, with periodic reviews to ensure the effectiveness of vulnerability management measures.

12.6.1.1.7 Collaboration with External Sources:

- The college shall establish mechanisms to obtain information about technical vulnerabilities from reliable external sources, enhancing its ability to stay abreast of emerging threats.

12.6.1.1.8 Training and Awareness Program:

- Regular training and awareness programs shall be conducted to educate staff and students about the importance of identifying and reporting technical vulnerabilities.

12.6.1.1.9 Documentation and Record-Keeping Policy:

- Comprehensive documentation shall be maintained regarding vulnerability assessments, risk evaluations, mitigation measures, and

response actions taken.

12.6.1.1.10 Compliance and Audit Protocol:

- Regular audits shall be conducted to ensure compliance with vulnerability management policies and procedures, with findings used to improve the effectiveness of the program.

12.6.2 Restrictions on software installation

To enforce the Restrictions on Software Installation Policy, the following procedures shall be established. The Software Installation Oversight Committee, chaired by the Chief Information Officer (CIO) and the Chief Administrative Officer (CAO), is responsible for ensuring the implementation of these procedures.

PROCEDURES

12.6.2.1 Guidelines

12.6.2.1 Authorized Software Installation:

- Only authorized personnel designated by the IT department are permitted to install software on company-owned devices.
- Users shall not install any software on company devices without obtaining prior approval from the IT department.

12.6.2.1.2 Software Approval Process:

- Before installing any new software, users must submit a request to the IT department detailing the purpose, source, and potential security implications of the software.
- The IT department will evaluate the software to ensure it complies with company policies, licensing agreements, and security standards.
- Upon approval, users will be provided with instructions for the installation process.

12.6.2.1.3 Prohibited Software:

- Users are prohibited from installing unauthorized or unlicensed software on company devices.
- Software obtained from unofficial sources, including peer-to-peer networks or unauthorized websites, is strictly forbidden.

12.6.2.1.4 Security Considerations:

- Users must ensure that the software being installed does not introduce security vulnerabilities or compromise the confidentiality, integrity, or availability of company data
- Users shall not bypass security controls or disable antivirus software during the installation process.

12.6.2.1.5 Patch Management:

- It is the responsibility of the IT department to regularly update and patch all installed software to address known vulnerabilities.
- Users must promptly install patches and updates provided by the IT department to mitigate potential security risks.

12.6.2.1.6 Monitoring and Compliance:

- The IT department reserves the right to monitor software installations and usage to ensure compliance with this policy.
- Non-compliance with this policy may result in disciplinary action, including but not limited to revocation of software installation privileges and possible termination of employment.

12.6.2.1.7 Software Inventory Management:

- The IT department shall maintain an up-to-date inventory of all approved software installations across company devices.
- Regular audits shall be conducted to ensure compliance with the approved software list and to identify any unauthorized installations.

12.6.2.1.8 Documentation and Records Management:

- The IT department shall maintain documentation for all approved software installations, including licensing agreements, installation instructions, and relevant support contacts.
- Records of software requests, approvals, installations, and updates shall be securely stored for audit and compliance purposes.

12.6.2.1.9 User Training and Awareness:

- Provide regular training sessions or resources to educate users on the importance of software installation policies, security best practices, and the potential risks associated with unauthorized software installations.
- Foster a culture of awareness and accountability among users regarding their roles and responsibilities in maintaining the security of company devices.

12.6.2.1.10 Software Removal Procedure:

- Define procedures for the removal of outdated, unused, or unauthorized software from company devices.
- Regularly review software installations to identify obsolete or redundant applications and initiate removal processes to maintain system efficiency and security.

12.6.2.1.11 Risk Assessment and Mitigation:

- Conduct regular risk assessments of installed software to identify potential vulnerabilities, threats, and security risks.
- Implement appropriate mitigation measures, such as network segmentation, access controls, or software restrictions, to minimize the impact of identified risks.

12.6.2.1.12 Continuous Improvement:

- Encourage feedback from users, IT personnel, and stakeholders to continuously improve the software installation policy and procedures.
- Regularly review and update the policy in response to emerging threats, technological advancements, and organizational changes.

12.7 Information systems audit considerations

To ensure effective Information Systems Audit Considerations, the following procedures shall be established. The Audit Planning and Coordination Committee, overseen by the Head of IT Operations and the Chief Compliance Officer, is responsible for ensuring the implementation of these procedures.

PROCEDURES

12.7.1 Guidelines

12.7.1.1 Planning and Agreement:

- **Meticulous Planning:** Before conducting any audit activities, thorough planning is essential. This includes determining the scope of the audit, identifying the resources needed, and establishing timelines.
- **Mutual Agreement:** It's crucial to ensure that all stakeholders involved in the audit process agree on the plan. This agreement should encompass the timing, scope, and objectives of the audit.

12.7.1.2 Risk Assessment:

- **Comprehensive Assessment:** A detailed risk assessment should be carried out to identify potential risks associated with the audit activities. This assessment helps in understanding the potential impact on operational systems and aids in devising appropriate mitigation strategies.

12.7.1.3 Communication and Coordination:

- **Clear Communication Channels:** Effective communication among all stakeholders involved in the audit process is vital. Clear channels of communication should be established to ensure that everyone is informed about the audit activities and their potential impact on operational systems.
- **Coordination Efforts:** Coordination efforts should be made to minimize disruptions. This involves collaborating with relevant departments to schedule audit activities, at times that least interfere with critical business processes.

12.7.1.4 Timely Scheduling:

- **Strategic Timing:** Audit activities should be scheduled at strategic times to minimize disruption to ongoing business operations. This includes avoiding peak operational periods and considering the availability of resources necessary for the audit.

12.7.1.5 Training and Awareness:

- **Personnel Training:** Personnel involved in audit activities should undergo training to understand the importance of minimizing disruptions to operational systems.
- **Awareness:** They should be made aware of their roles and

responsibilities in achieving this objective and ensuring the smooth functioning of business processes during audits.

12.7.1.6 Continuous Improvement:

- Feedback Utilization: Feedback obtained from audit activities should be carefully analyzed and used to implement improvements in the process.
- Continuous Monitoring: Continuous monitoring of the effectiveness of measures taken to minimize disruptions should be conducted to ensure ongoing improvement.

12.7.1.7 Compliance Monitoring:

- Regular Monitoring: Regular monitoring and review of compliance with the policy should be carried out to ensure adherence to ISO 27001 standards and organizational objectives.
- Compliance Review: This includes checking whether the planned audit activities align with the agreed-upon procedures and whether any deviations require corrective action.

12.7.1.8 Documentation and Records:

- Documented Evidence: All audit plans, agreements, risk assessments, communication records, and improvement actions should be documented and maintained as evidence of compliance.
- Records Retention: These records serve as a reference for future audits and provide evidence of the organization's commitment to minimizing disruptions during audit activities.

12.7.1.9 Responsibilities:

- Defined Roles: Clear roles and responsibilities should be defined for personnel involved in implementing and adhering to the policy.
- Accountability: This ensures accountability for ensuring the smooth conduct of audit activities with minimal disruption to operational systems.

12.7.1.10 Review and Approval:

- Periodic Review: The policy should be periodically reviewed to ensure its alignment with organizational goals and ISO 27001 standards.
- Management Approval: Approval from relevant management authorities should be obtained to endorse any changes made to the policy.

12.7.1.11 Enforcement:

- Disciplinary Measures: Non-compliance with the policy may result in disciplinary action, as per organizational policies and procedures.

- Upholding Integrity: This ensures the integrity of information security and operational continuity by enforcing adherence to the policy.

12.7.1.12 Policy Maintenance:

- Regular Updates: The policy should be maintained and updated as necessary to reflect changes in organizational structure, processes, or regulatory requirements.
- Relevance and Effectiveness: This ensures that the policy remains relevant and effective in addressing the organization's needs and objectives related to minimizing disruptions during audit activities.