**Pennsylvania College of Technology**

**Information Security Policy**

Jeffrey Yang

**Table of Content**

Audit and Accountability (AU) 3

Security Assessment and Authorization (CA) 8

System and Information Integrity (SI) 13

Risk Assessment (RA) 19

Incident Response (IR) 24

System and Services Acquisition (SA) 30

Configuration Management (CM) 36

Contingency Planning (CP) 42

Awareness and Training (AT) 48

Data Encryption (UNOFFICIAL) 52

Implementation Date: 05/07/19 Control Area: Information System

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain an Audit and Accountability (AU) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. The policy will help aid in identifying accidental disruption, tampering, damage, or other forms of potential incidents that would compromise the confidentiality, integrity, and availability of the College’s information systems. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy whenever an audit is done on the information systems or annually for review and/or changes.

Purpose:

The purpose of this policy is to ensure the confidentiality and integrity of information systems of the College’s information system infrastructure, hardware and software and protect it from a wide range of threats, internal and external. It will aid in the detection of abnormalities in the information system and actions needed to protect against such threats and future additional security implementations as seen fit.

Audience:

The policy will primarily be for, but not limited to, the information technology staff on the College campuses, executives for possible mission critical decisions, the legal team in the case of legal issues, as well as PCT’s security staff.

Policy:

Each campus under the College must comply and follow a formal, documented program to assess, report, adjust, and retain audits done on their information systems in order to ensure best practices and the following of baselines.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met or whenever there is a change in the information system. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the system will be maintained through, but not limited to automated audit reporting systems, audit reports, audit information storage, audit failures, and audit information retention.

The following mandatory controls are College-wide controls that are to be implemented, in use, and in continuous improvement. They are derived from the AU controls described in the NIST SP 800-53 (Rev. 4). The College and each campus must establish and maintain the following controls:

1. Audit Events (AU-2): PCT’s IST team will be in charge of monitoring and assessing any observable occurrences within audit events that may cause an issue to the security of the information system. Auditable events will be established within the auditing policy within the system, and may consist of but not limited to: startup and shutdown of servers, account logins, objects accessed in the system, account creation and deletion, and account privilege changes. Observations of audit events will not just be limited to a single information system but through all information systems that PCT owns and operates such as email servers and website servers. Audit events observation may be applicable to other entities within PCT and can be determined by the IST manager as he/she determines the security risks associated with that entity towards the information system. Additional audit events may be added to the observation list through the approval of the IST manager, and with a rationale behind how it would affect the security of the information system.
2. Content of Audit Records (AU-3): The information system will generate additional information alongside the audit reports that may be important to analysts and the IST team and manager. The information included with these reports should include but are not limited to: time stamps for logins, modifications, shutdown/startup of servers, source and destination addresses, event descriptions, success/fail indications, file names involved, and access control or flow control rules invoked. Additional contents to the audit reports may be added by the IST manager through a rationale involving how it would affect the security of the information system.
3. Audit Storage Capacity (AU-4): The College will retain ample storage capacity for audit records determined by the IST manager at the time. Additionally, a backup storage unit will be kept with records on file in the case of an incident that would cause damage to the original storage unit.
4. Response to Audit Processing Failures (AU-5): The information system will be set up with a method to alert the IST team about audit failures by means of on-screen alerts, sounds, or methods such as e-mail. Once a failure is detected and the IST team is alerted, an audit report should be generated by the information system, and if not, it should be done by the IST team manually. The report will be consistent of all contents outlined in AU-3. Normal operations can begin immediately in the case of a false alert. Whether false positive or positive audit failure is detected, the information system will be equipped with a tool to prevent further audit processes until the issue is resolved. Actions taken against the audit failure will be determined by the severity of the failure as outlined by the IST manager. These failures will require the decision made by the IST manager to determine the actions necessary to reduce or prevent damage to the information system. The options granted to the IST manager to prevent damages due to an audit failure may include but are not limited to: shutting down the information system, stoppage of the generation of audit records, stoppage of audit processes, and a rollback from backup storage to the most recent audit record.
5. Audit Review, Analysis, and Reporting (AU-6): PCT’s IST team will be tasked with reviewing and analyzing the information system’s audit records daily for discrepancies in the audit events that the information system is not set to alert or failed to create an alert. These discrepancies are listed but not limited to the audit events in AU-2. All events will be reviewed and analyzed for security threats against the information system. Once analyzed and reviewed, a report will be generated and provided to the IST manager for further review, to which he/she will determine further actions as outlined in AU-5 in the case of audit failures. In addition, audit events that may have an impact on mission critical processes will be further reported to the college executives for appropriate actions to be made.
6. Audit Reduction and Report Generation (AU-7): The information system will produce an audit reduction and report generation that supports audit reviews, analyses, and reports after the case of an incident which does not alter the original content or time ordering of the audit records for the IST manager and staff to analyze easier. This will be included into the audit report as well.
7. Time Stamps (AU-8): The information system will use an internal clock to leave a time stamp including the date and time on every audit record. The times will be recorded in UTC and GMT.
8. Protection of Audit Information (AU-9): The information system will protect audit information from unauthorized personnel who may try to gain access, modify, or delete files and contents. Audit information included but are not limited to: audit records, audit reports, audit time stamps, and audit backup storage. The IST manager will be the only personnel granted authorization to the audit information, through which he/she can share the information if needed, but must be done through him/her.
9. Audit Record Retention (AU-11): The information system will retain audit records for a minimum of three years after being generated before deletion. This will allow insight on issues in the future that may have occurred in the past and for legal issues in the case of an incident involving an audit event.
10. Audit Generation (AU-12): The information system will provide audit record generation for the events outlined in AU-2 and contents outlined in AU-3 including but not limited to software, hardware, and network. The system also grants the IST manager at the time the ability to choose which auditable events are to be audited by specific components of the information system.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system staring from its inception all the way until it is resolved. Documentation of the exception must be made an may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may break policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives deem that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the ‘Human Resources Management Policy.’

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

IST – Information Systems and Technology

Revision History:

05/07/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Information System

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain a Security Assessment and Authorization (CA) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. The policy will promote a secure environment for the information system through security controls and authorization of roles within the system. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to ensure the confidentiality, integrity, and availability of PCT’s information system infrastructure, hardware and software; protecting it from internal and external threats. The policy will aid in establishing proper guidelines and procedures for the authorization of personnel and services that affect the information system as well as guidelines in the assessment of the system for possible issues that could cause damage it. The authorization and assessment process will be continuously applied in due necessity in the cases of role changes or any change within the information system. Keeping authorization and assessments up to date will reduce the likelihood of the information system being compromised through possible threats.

Audience:

The policy will primarily be for, but not limited to, the information technology staff on PCT campuses, executives for possible mission critical decisions, and the legal team in the case of legal issues.

Policy:

Each campus under PCT must comply and follow a formal, documented program to assess and report discrepancies that could be a possible threat or vulnerability within the information system that could lead to a breach of confidentiality, integrity, and availability. The documented program will provide means of authorizing roles and assessment processes.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met or whenever there is a change in the information system. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the system will be maintained through, but not limited to the development of a security assessment plan and authorization process; system milestones and monitoring; as well as internal communications for PCT’s information system.

The following controls are college-wide and to be implemented, in use, and in continuous improvement. They are derived from the CA controls described in the NIST SP 800-53 (Rev. 4). Each campus under PCT must establish and maintain the following controls:

1. Security Assessments (CA-2): PCT’s IST team will be tasked with assessing the security of products or services used or produced by the information system. Within the assessment plan, the team will be responsible for evaluating the security controls and their effectiveness as well as the environmental factors such as personnel who can access the system as well as their roles and responsibilities. This assessment will be done on an annual basis and every time the information system is updated or changed. The assessment will conclude in the form of a written report by the IST team and delivered to the IST manager for review.
2. System Interconnections (CA-3): The IST team will be responsible for authorizing connections between PCT’s information system and other information systems through the use of Interconnection Security Agreements. The team will be tasked with implementing PCT’s security policies for their information system to any outside information system that it is to develop a connection with. Other information systems thus must comply to the security policies that PCT applies to their information system. The Interconnection Security Agreements will be reviewed and updated annually or if there is a change to the security policies affecting the information system.
3. Plan of Action and Milestones (CA-5): The IST manager will work with the IST, Incident Response, and Contingency Planning team in developing actions taken in the case of attacks or damages done to the information system through the correction of weaknesses, patching of vulnerabilities, or implementation of an incident response or contingency plan in case of disasters. Documentation of planned actions will be developed by the IST manager as well as the corresponding members, such as the contingency team with the contingency plan respectively. The development and updates to the information system will discussed as well annually to reflect the mission of PCT.
4. Security Authorization (CA-6): The IST manager will be assigned to the be the authorizing official for the information system. All processes and operations dealing with the information system must be authorized by the IST manager before it can be implemented. The security authorization will be updated annually or if there is a change in the authorizing official.
5. Continuous Monitoring (CA-7): The IST team and manager will be responsible for establishing and implementing a continuous monitoring program consisting of software, hardware, and personnel on duty. High risk systems or services should be monitored, such as but no limited to vulnerable network ports, mission critical functions, and system log files for discrepancies that could lead to an attack. Monitoring software and hardware will be run as long as the information system is up, and personnel will be on duty during business hours, but may be contacted by the information system in the case of mission critical emergencies caused by the system. Continuous monitoring will undergo security assessments and authorization as outlined in CA-2 and CA-6. The IST team will further analyze issues that may arise from the monitoring and generate a report to which will be delivered to the IST manager for review and determining a course of action.
6. Penetration Testing (CA-8): PCT will enlist penetration services provided by third party organizations that specialize in penetration testing to test the information system for possible vulnerabilities as well as having an internal penetration testing team. A meeting with the IST manager and college executives along with the service provider will be conducted to outline the goals of the penetration test as well as parameters. A penetration test will be conducted quarterly by PCT’s internal penetration testing team or whenever the information system is updated that may result in possible mission critical issues if breached. A third-party service will be required to assess the entire information system annually.
7. Internal System Connections (CA-9): Authorization of internal connections for PCT owned devices that connect to the information system or network such as computers, printers, servers, etc., must be established initially before operation. Security requirements of these devices are as listed in PCT’s security policy.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system staring from its inception all the way until it is resolved. Documentation of the exception must be made an may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may break policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives deem that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the ‘Human Resources Management Policy.’

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

IST – Information Systems and Technology

Revision History:

05/07/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Information System

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain a System and Information Integrity (SI) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. The policy will help aid in identifying threats against the College’s information system that could cause disruptions in the daily functions of the College as well as the integrity of the information on the system. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to ensure the integrity and availability of the information systems of the College’s information system infrastructure, hardware and software and protect it from threats ranging from internally or externally. The policy will aid in the detection of threats and changes aimed and applied to the information system so appropriate action can be taken to protect it. Future security measures could be implemented as deemed fit to further protect the information system.

Audience:

The policy will primarily be for, but not limited to, the information technology staff on the College campuses, executives for possible mission critical decisions, the legal team in the case of legal issues, as well as students and staff as the integrity of College information directly affects day to day processes.

Policy:

Each campus under the College must comply and follow a formal, documented program to asses and report discrepancies within the information system that could lead to a breach of information integrity and availability.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met or whenever there is a change in the information system. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the system will be maintained through, but not limited to the restoration of faults and vulnerabilities, malicious codes against the system through monitoring as well as other software, integrity of software and hardware components as well as communication services, and handling of errors and validation of information inputs.

The following controls are College-wide and to be implemented, in use, and in continuous improvement. They are derived from the SI controls described in the NIST SP 800-53 (Rev. 4). The College and each campus must establish and maintain the following controls:

1. Flaw Remediation (SI-2): PCT’s IST team will identify, correct, and report on flaws in the information system that may be derived from system updates, patches, or a malicious external or internal source. The team will report directly to the IST manager appointed at the time. Other controls to enforce flaw remediation will include:
   1. The testing of software and firmware updates or fresh installs for potential side effects including effectiveness of the product and issues that could cause harm before installation.
   2. Updates of security related software and firmware must be tested within one week of it’s release in a simulated environment such as a sandbox or virtual machine. Flaw remediation will continue through the process of configuring the update for any additional issues that could arise before the actual installation into the College’s information system.
2. Malicious Code Protection (SI-3): PCT’s IST team will implement protection mechanisms such as an antivirus software on the information system’s entry and exit points to detect and eliminate malicious code. Entry and exit points include but are not limited to: firewalls, electronic mail servers, web servers, computers, and mobile devices. Malicious code can consist of but are not limited to: viruses, worms, Trojan horses, spyware, and ransomware.
   1. Updates to malicious code protection mechanisms should be tested and updated immediately but must go through the procedure and time period outlined in SI-2 as it is a security related software.
   2. The malicious code software will be configured to do automatic scans of the information system on a weekly basis and real-time scans of files on all open ports where files are downloaded, opened, or executed. An exception to the automatic scans is if an IST team member or the IST manager has reason to do a scan due to discrepancies in the information system that could point towards malicious code inside.
   3. If malicious code is discovered on the system, the malicious code will be quarantined and the information system will block information system activities. The IST manager appointed at the time will be alerted. Unaffected sections of the information system will be brought back to a running state once deemed safe. The affected parts will remain down until the malicious code is addressed and remediated.
3. Information System Monitoring (SI-4): PCT’s IST team will continuously monitor the information system to detect potential attacks through indicators as outlined in AU-2 in the Audit and Accountability policy. These include but are not limited to: startup and shutdown of servers, account log-ins, objects accessed in the system, account creation and deletion, and account privilege changes. Other indicators may also include unauthorized local, network, and remote connections.
   1. Unauthorized use of the information system will be identified through the use of indicators listed in the previous statement. Additional methods would include the IST team using a SIEM (security information and event management) software and an intrusion detection and prevention software.
   2. Monitoring devices will be deployed to mission critical locations and their path to discover potential attacks before it occurs; as these locations have an increased risk to the College’s daily operations.
4. Security Alerts, Advisories, and Directives (SI-5): PCT’s IST team will continuously receive security alerts, advisories, and directives from external organizational services related to the information system and will generate reports on the security alerts, advisories, and directives as deemed necessary. The security alerts, advisories, and directives will be dispersed to the IST manager appointed at the time and they will decide whether to implement security directives within the established time frame or notify the external organization of the degree of noncompliance.
5. Software, Firmware, and Information Integrity (SI-7): PCT’s IST team will employ and monitor integrity verification tools to detect unauthorized changes to software, firmware, and information. Software consist of things such as operating systems and applications. Firmware include BIOS (Basic Input Output System). Information consists of metadata associated with information. The IST team will implement and use alongside of integrity verification tools, but also parity checks, which will allow basic error detection.
   1. SI-7(1): The College’s IST team will run integrity checks on transitional states such as system startups, restarts, shutdowns, and aborts. Installation of new hardware, software, or firmware must run through SI-2 before installation.
   2. SI-7(2): The information system will automatically report to the IST team and manager of integrity violations through the use of an automated tool. This will effectively reduce the time needed to fix the issue, especially if it affects mission critical sections of the information system.
6. Spam Protection (SI-8): PCT’s IST team will implement spam protection mechanisms at information system entry and exit points to detect and remediate unsolicited messages. Updates to the spam protection mechanism will be made but has to follow SI-2.
   1. In addition to the spam protection mechanism, monitoring will be focused on the electronic mail communication as that is the likeliest target of spam messages. Confidentiality of student and staff information such as passwords could be stolen through phishing e-mails. Messages coming in and out should be monitored for spam. This will not be a breach of policy as the College provides the e-mail addresses based on their own Internet domain.
7. Information Input Validation (SI-10): The information system will check the validity of inputs on web services. The College has a search bar on their public website which could allow the possibility of a cross-site script attack or injection attacks such as a SQL injection.
8. Error Handling (SI-11): The information system will generate error messages and reports them to the IST manager appointed at the time who will determine corrective actions to be taken to resolve the issue without reveling information that couple help attacks exploit the vulnerability in the information system. Error messages will be sent but not limited to when logon attempts fail, or unsuspected system shutdowns.
9. Information Handling and Retention (S-12): PCT’s IST team handles and retains information within the information system for however long the ITS manger, college executives, and legal team deem a reasonable time before deleting them. Holding on to the information will provide insight on issues that may have occurred before and for legal issues in the case of an incident.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system staring from its inception all the way until it is resolved. Documentation of the exception must be made an may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may break policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives deem that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the ‘Human Resources Management Policy.’

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

IST – Information Systems and Technology

SIEM – Security Information and Event Management

SQL – Structured Query Language

Revision History:

05/07/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Information System

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain a Risk Assessment (RA) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53), Revision 4. The policy will help aid in identifying risks against the information system and the course of action taken against those risks that could cause disruptions in the daily functions of the college as well as the confidentiality, integrity, and availability of the system. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to ensure the confidentiality, integrity, and availability of the information system of PCT’s information system infrastructure, hardware and software and protect it from threats ranging from internally to externally. The policy will aid in detection of risks and outlines the course of action to be taken in the case that a risk becomes an issue that would require immediate attention. As risk is defined as the intersection between threats, assets, and vulnerabilities, we need to be continuously improving in the security of these fields to reduce our risk.

Audience:

The policy will primarily be fore, but not limited to, the information technology staff on PCT campuses, executives for possible mission critical decisions, the legal team in the case of legal issues.

Policy:

Each PCT campus must comply and follow a formal, documented program to assess and report discrepancies that could be a possible threat or vulnerability within the information system that could lead to a breach of confidentiality, integrity, and availability.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met or whenever there is a change in the information system. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the system will be maintained through, but not limited to the categorization of security risks against the system as well as a risk assessment plan that will identify and analyze the impact of the risk against the information system.

The following controls are college-wide and to be implemented, in use, and in continuous improvement. They are derived from the RA controls described in the NIST SP 800-53 (Rev. 4). PCT and each of its campuses must establish and maintain the following controls:

1. Security Categorization (RA-2): PCT’s IST team will be responsible for categorizing information as well as the entire information system in accordance to risk assessment procedures, as outlined in the “Risk Analysis and Threats,” security document. Additional requirements of this control include:
   1. Documentation of the information categorization results will be reviewed by the IST manager and approved to which it will be made only available to the IST manager, risk assessment team, and college executives in control of mission critical decisions. The purpose of documentation allows PCT’s risk assessment team to have information, not necessarily of the risks, but the components that create risk, which include assets, vulnerabilities, and threats, which will assist the risk assessment team in generating the level of risk posed against PCT’s information system accurately.
2. Risk Assessment (RA-3): PCT’s IST will provide documentation of activities and information about the information system and present the results to the risk assessment team. Assessment of the risk will be conducted to determine the magnitude of harm that could occur to the college’s daily operation and information system.
   1. The risk assessment team will take the documentations provided by the IST team as outlined in Control 1 in the current policy. The level of risk will be determined through the security aspects of these three categories: assets, vulnerability, and threat. The affects of each against the college and its operations are listed:
      1. Assets; in which in the college’s case, is information assets that include but are not limited to student/staffs’ full names, home addresses, and phone numbers.
      2. Vulnerability; or exploitable weaknesses within the information system, which is what PCT’s security policies are focused on, through the use of continuous monitoring of the information system as outlined in Control 3 in the ‘System and Information Integrity’ Policy as well as Control 1 in the ‘Audit and Accountability’ Policy.
      3. Threat; which are the attackers of a vulnerability in our system. This is not only limited but can include Advanced Persistent Threats (APT) by which the IST team will categorize if the occasion ever occurred.

These components of risk will assist the risk assessment team in generating the level of risk posed against PCT’s information system accurately.

* 1. The risk assessment results produced by the risk assessment team will disseminated to the IST manager and college executives to determine the best course of action to take against the risk. The legal team will also be notified so the legal positions can be provided to help aid in decision making.
  2. The risk assessment team will not only be in charge of determining the risk, but also when prompted, to produce possible courses of actions to be taken in the case the risks are happen to occur. The risk assessment team will look at a few possible ways to deal the risk:
     1. Avoidance; the best-case scenario in which is the purpose of the college’s security policies. PCT’s information assets will be safe if the risks never materialize and cause damage.
     2. Mitigation; if risk were to materialize, a course of action must be taken in order to attempt and mitigate it so damage to the system is reduced to a minimum. This will be decided by the IST manager and risk assessment team during the occurrence because of a risk’s nature, in which we are unable to fully predict it.
     3. Transfer; the college will be partnered with a third-party organization that deals with exploited or compromised systems and call upon their services if the damage cannot be properly mitigated.
     4. Acceptance; this is the last possible solution as we can only allow the damage to run its course until it is stopped. An exception to this is if justified and given proper instructions by the college executives, the IST manager can stop the function of the information system if it could help reduce damage.
  3. The risk assessment documents and policy will be updated annually or whenever there is a significant change to the college’s information system that could present an increased or new form of risk such as the identification of new threats or storage of more information assets due to possible college expansions into new fields, etc.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system staring from its inception all the way until it is resolved. Documentation of the exception must be made an may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may break policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives deem that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the ‘Human Resources Management Policy.’

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

IST – Information Systems and Technology

Revision History:

05/07/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Incident Response

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain an Incident Response (IR) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. The policy will help aid in assessing and generating a course of action against the possibility of and occurrence of an incident against PCT’s information system that could cause disruptions in the daily functions of the college as well as the confidentiality, integrity, and availability of the system. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to ensure the confidentiality, integrity, and availability of PCT’s information system infrastructure, hardware and software; protecting it from internal and external threats. The policy will aid in detection of signs of an incident and outlines the course of action to be taken in the case that an incident occurs and would require immediate attention. Incidents can be caught in its early stages through detection of anomalies within the system and would require training. PCT will continuously be improving training and awareness amongst staff members that work with or around the information system to improve the likelihood of an incident being caught and dealt with in its inception. If that is not the case, then staff is also trained in the event of an incident.

Audience:

The policy will primarily be for, but not limited to, the information technology staff on PCT campuses, executives for possible mission critical decisions, and the legal team in the case of legal issues.

Policy:

Each campus under PCT must comply and follow a formal, documented program to assess and report discrepancies that could be a possible threat or vulnerability within the information system that could lead to a breach of confidentiality, integrity, and availability. The documented program will also provide a means of training staff members in the event of an incident.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met or whenever there is a change in the information system. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the system will be maintained through, but not limited to the training of staff to recognize discrepancies/events that could lead to an incident, the handling of the incident through monitoring and reporting, as well as an outlining an incident response plan for PCT’s information system.

The following controls are college-wide and to be implemented, in use, and in continuous improvement. They are derived from the IR controls described in the NIST SP 800-53 (Rev. 4). Each campus under PCT must establish and maintain the following controls:

1. Incident Response Training (IR-2): PCT’s IST manager will be responsible for establishing and promoting an incident response training course. The incident response team will require formal training within 30 days of being hired to complete an incident response training proctored by the IST manager or an assigned trainer by the IST manager. In addition to the incident response team being trained, other staff members that deal with the information system on a day to day basis such as the IST team will also require training but a less rigorous one that needs to be completed within 30 days of hire. Another condition that must be met is that an incident response training will be done when the information system changes, and annually thereafter. Training will be outlined by the IST manager and may consist of but are not limited to:
   1. Recognition of an incident on an information system.
   2. Recognition of suspicious activity internally or externally that could lead to an incident.
   3. How to handle/remediate the incidents.
   4. Personnel to contact in the case of an incident.
2. Incident Handling (IR-4): The incident response team will be responsible for incident handling in the case of information about and the occurrence of an incident. Responsibilities will include detection of an incident, which can be from anyone that has been trained under the IR-2 control, but once detected, if it is staff besides the incident response team, it will be handed over to the incident response team for further analysis, containment, eradication, and recovery. Information discovered pertaining to the incident of the information system will directly affect contingency planning activities related to the information system. Final reports after the incident has been dealt will be given to the IST manager at the time to incorporate into future incident handling cases, incident plans, and training to help prevent a similar incident to occur.
3. Incident Monitoring (IR-5): The incident response team will be responsible for tracking and maintaining documents on previous, possible, and occurring incidents. The incidents will be documented not only for report purposes, but also as future training material created by the IST manager in providing better training for those responsible for incident response for the college’s information system. Documentation will be able to be used by the PCT’s legal team in the case of legal issues for evidence. Things that are included in these documents span to other policies, including:
   1. Audit and Accountability Policy; control AU-6.
   2. Systems and Information Integrity Policy; control SI-4.

In addition to monitoring, the incident response team will use tools that calculate the severity level of the incident when monitoring them. The incident levels will be broken into 5 severity levels where SEV stands for severity:

* SEV-1: Critical issues in the information system that requires public notification and meeting with the college’s executive board and immediate attention.
* SEV-2: Critical issues in the information system that would impact the ability of users to use the services of the information system and require immediate attention.
* SEV-3: Minor issues in the information system that impact users of the information system and require immediate attention.
* SEV-4: Minor issues in the information system that does not affect users but requiring action.
* SEV-5: Minor issues in the information system such as bugs that do not affect users.

1. Incident Reporting (IR-6): The incident response team and other staff members that work with the information system that had undergone training listed in IR-2 will have 24 hours to report a suspected security incident to the IST manager. From there, the IST manager will implement the incident response plan as outlined in IR-8.
2. Incident Response Assistance (IR-7): PCT’s executives will permit the assistance of other groups to work under the IST manager, who is the one responsible to rolling out the incident response plan. Assistance can range from IT help desks including the student help desk and the help desk in the computer lab in the Klump Academic Center to the network manager. Access to older incidents that may be held by the legal team can be accessed too.
3. Incident Response Plan (IR-8): PCT’s IST manager will develop an incident response plan with the assistance of the incident response team in the case of an incident in the information system. The incident response plan will consist of:
   1. Overview of the incident will be reviewed by the IST manager and the incident response team along with all reports and monitoring leading up to the point of the incident. Classification of severity level of the incident will follow the guideline provided in IR-5. The team will develop the safest and most effective method to deal with the specific incident depending on its characteristics. All final decisions will be made by the IST manager before implementation. The goal of this step will create:
      1. Acknowledgement of the incident having occurred.
      2. Examination of the incident and best method to control it.
      3. Development of action geared towards the specific incident.
      4. Implementation of the incident and expectation.
   2. PCT does not have a group of staff specialized only in incident response due to the reason that the information system is not at a high risk along with the fact that our IST staff is able to manage most small incidents, but are trained to deal with large incidents if the case arises. If the incident persists and the IST manager deems it out of our expertise, third party services may be called upon to assist in the matter.
   3. All incidents must be reported and documented. Suspecting of an incident must be reported but if no incident comes from it, then it does not need to be documented.
   4. Assistance from other staff will be given to the IST manager by the executives as needed for them to roll out the incident response plan according to control IR-7.
   5. All additional steps and actions to stop the incident from progressing must be reviewed and approved by the IST manager, unless it is mission critical, then approval from the college executives must be granted as well.

The incident response plan will then be distributed to all IST staff members as well as the college executives to understand the method and approach being taken to restore the information system to its original state. Additional staff may be given the incident response plan depending whether they are to provide assistance to the incident response team or not outlined in control IR-7.

The incident response plan will be reviewed annually unless there is a change in the information system or an incident occurs. Updates to the incident response plan will be done in accordance to an incident or a change in the information system. Changes to the incident response plan can only be made by the IST manager at the time and reported to college executives. The incident response plan will be protected from unauthorized disclosure and modification.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system staring from its inception all the way until it is resolved. Documentation of the exception must be made an may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may break policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives deem that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the ‘Human Resources Management Policy.’

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

IST – Information Systems and Technology

Revision History:

04/14/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Information System

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain a System and Services Acquisition (SA) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. The policy will help aid in assessing the security requirements of the development and acquisition of hardware, firmware, and software for PCT’s information system to protect its confidentiality, integrity, and availability. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to ensure the confidentiality, integrity, and availability of PCT’s information system infrastructure, hardware and software; protecting it from internal and external threats. This policy will aid in assessing the life cycle of the information system, incorporating security from its inception and throughout its useful life. Security measures will be administered against all parts of the system development life cycle, including the updating of the system through firmware, hardware, or software in the case of either confidentiality, integrity, or availability being compromised and requiring immediate attention. When security is implemented through every stage of a system’s life cycle (SDLC), it is more likely to be secure, through stronger security practices. PCT will continuously be improving the security of the information system through best security practices, through the educating and training our IST team to be more aware to issues in the information system so it can be dealt with in a timely manner.

Audience:

This policy will primarily be for, but not limited to, the information technology staff on PCT campuses, executives for possible mission critical decisions, the legal in the case of legal issues, as well vendors that work with PCT directly, as their products/services must match and abide by PCT’s security policy.

Policy:

Each campus under PCT must comply and follow a formal, documented program that addresses best security practices when it comes to introducing new firmware, software, hardware and general processes throughout the SDLC. The documented program will also provide means of training staff member to recognize and administer best security practices when working with the information system.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met or whenever there is a change in the information system. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the system will be maintained through, but not limited to the testing of new firmware, software, and hardware, the allocation of resources for system acquisitions, documentation of the information system, and the application of security throughout the entirety of the SDLC.

The following controls are college-wide and to be implemented, in use, and in continuous improvement. They are derived from the SA controls described in the NIST SP 800-53 (Rev. 4). Each campus under PCT must establish and maintain the following controls:

1. Allocation of Resources (SA-2): PCT’s IST team and manager will request a budget for the allocation of financial resources for upgrades to the information system that could form in but not limited to firmware, software, hardware, and personnel. Funding will be set aside to keep the regular maintenance and operation of the information system. The IST manager and team will determine what additional upgrades are more critical than others for PCT’s financial team to develop a proper budget.
2. System Development Life Cycle (SA-3): The management of the information system will be administered by the IST team through a seven-step process to meet the requirements of a secure SDLC. Security will be implemented in every step of the SDLC. The steps consist of:
   1. Planning; through which the IST manager and IST team will determine the necessary path to take the information system whether through replacement of older software or hardware, or the impact of a new update.
   2. System Analysis & Design; the IST manager and IST team will go through an analysis of the information system in determining what is the most necessary changes and list them by level of importance.
   3. Systems Design; larger scale changes to the information system may require the IST manager and IST team to require more resources as the need to remodel/re-design the information system may be required. After this, the IST team and IST manager can create a request for budget by the college.
   4. Development; the development of the information system would consist of the receiving of the firmware, software, hardware or updates. The installation of the new wares or updates will be done on a virtual machine first.
   5. Integration & Testing; the IST team will integrate and test the new firmware, software, hardware or updates through the testing environment to see if there are any security issues. This entire process will be over seen by the IST manager and relates to control 1, (SI-2), in the System and Information Integrity Policy.
   6. Implementation; the IST team will then implement the new firmware, software, hardware or update to the information system if it meets security requirements. This process will be over seen by the IST manager.
   7. Operations & Maintenance; the new firmware, software, hardware or updates will be put into operation within the information system and maintenance will need to be done. Monitoring of the new wares and updates in the system will be done, as outlined in control 5, (SI-7), in the System and Information Integrity Policy.

The IST team will be trained by the IST manager on security best practices and how they should be implemented in every step of the SDLC to ensure maximum security. The IST manager will have a role and over sees every process of the SDLC, from the planning of obtaining a new firmware, software, hardware or update to the end process and maintenance of the information system as a whole.

1. Acquisition Process (SA-4): PCT requires their IST manager and IST team to implement PCT’s security policies, standards, and guidelines to the acquisition of a new product or service for the information system. The requirements include:
   1. Security functional requirements; the new product or service is able to or willing to demonstrate the ability to produce security measures throughout its product/service, including the entirety of the SDLC of that specific product/service.
   2. Security-related documentation requirements; the proper documentation of implemented security best practices throughout the information system product/service is required as well as the use of security throughout the SDLC. Documentation will be reviewed by the IST manager.
   3. Requirements for protecting security-related documentation; protection of security-related documents must be implemented through the acquisition process, as disclosure of the type of services/products used for the information system could cause issues if that information was to be obtained by adversaries.
   4. Description of the information system development environment and environment that the product/service is to operate on is required for documentation and procedure processes. This is also required for PCT’s own SDLC of the implementation of the product/service.
2. Information System Documentation (SA-5): PCT’s IST team will document all aspects of the information system that relates to the SDLC, including the secure installation, configuration, and operation of components and services used/installed on the information system. Documentation of the procedures used to administer proper security controls in every phase of the SDLC process as well as all vulnerabilities discovered, through the testing process or implementation process. User documentation will be produced by the IST team as well, including security controls placed on users and their access abilities, interaction method between the system and user, as well as user contribution to the security of the information system. Documents will be protected as outlined in control 2, (RA-3), in the Risk Assessment Policy. Documentations will be distributed to the IST manager for information system related actions, college executives for mission critical reasons, as well as the legal team to hold on to in the case of a legal issue.
3. Security Engineering Principles (SA-8): PCT will require the IST team and manager to implement levels of security when developing or designing new updates to the information system. This applies to all phases of the SDLC outlined in control 2, and control 1 when dealing with the actual firmware, software, hardware or updates. The methods of securing the system will be determined and defined by the IST manager and may include but not limited to: the use of layered security; establishing procedures when using different areas of the information system; establishing physical and logical boundaries for the information system users.
4. External Information System Services (SA-9): PCT’s IST team and manager will be in charge of overseeing the security controls of external third-party information system services. The security controls applicable will be derived from this policy as well as the other security policies, standards, regulations, and guidelines. The external service must be able to provide documentation of the SDLC of their product/services to the IST manager for review for possible security deficiencies deemed by PCT’s security policies as outlined in control 2 in the current policy. The external service must adhere minimally to PCT’s security policies as it creates a consistent basis of security on which PCT can operate on.
5. Developer Configuration Management (SA-10): PCT will require the IST team to work beside the developer of the information system throughout the entire SDLC process starting at implementation and ending at operation if using an external service. If the development was internal, the IST manager and team will be required to provide configuration management throughout the entirety of the SDLC. Documentation of the management of the information system and changes to the system will be required as well as the tracking of security flaws and their remediation. Reports are to be generated as well.
6. Tamper Resistance and Detection (SA-18): PCT will require the IST team to monitor the tampering of the information system, its components, or services. Monitoring of firmware, software, and hardware will be administered as outlined in control 5, (SI-7), of the System and Information Integrity Policy.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system starting from its inception all the way until it is resolved. Documentation of the exception must be made and may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may not abide by policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives and IST manager come to a conclusion that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the “Human Resources Management Policy.”

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

IST – Information Systems and Technology

SDLC – System Development Life Cycle

Revision History:

05/07/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Configuration Management

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain a Configuration Management (CM) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. The policy will help aid in producing a configuration baseline and guidelines for the information system so possible anomalies or changes within the system that could cause damage to the infrastructure can be detected as well as disruptions to the daily functions of the college and the confidentiality, integrity, and availability of the system. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to ensure the confidentiality, integrity, and availability of PCT’s information system infrastructure, hardware and software; protecting it from internal and external threats. This policy will aid in outlining a basis for configuration methods as well as an established baseline to which changes can be compared to for analysis. Changes could create issues that include minor mistakes to crucial problems affecting mission critical components of the system that would require immediate attention. Establishment of configuration guidelines will impact the security of the system through controls and analysis. PCT will continuously be improving the configuration controls on the system through continual updates. Through these configuration controls and guidelines, we can reduce the likelihood of a configuration level security issue to occur.

Audience:

The policy will be for, but not limited to, the information technology staff on PCT campuses, executives for possible mission critical decisions, and the legal team in the case of legal issues.

Policy:

Each campus under PCT must comply and follow a formal, documented program to implement and maintain configuration controls including the establishment of a system baseline for the purpose of discovering and reporting discrepancies that could be a possible threat to the information system leading to a breach of confidentiality, integrity, and availability.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met or whenever there is a change in the information system. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the system will be maintained through, but not limited to the establishment of a configuration baseline for comparison purposes, change controls to grant permission or denial of changes to the system, restricted system functionality, and established configuration management plan.

The following controls are college-wide and to be implemented, in use, and in continuous improvement. They are derived from the IR controls described in the NIST SP 800-53 (Rev. 4). Each campus under PCT must establish and maintain the following controls:

1. Baseline Configuration (CM-2): PCT’s IST team and manager will be responsible for establishing a baseline configuration for the information system appropriate for its functions. Baselines will be created when the system is updated whether through hardware, software, or firmware, or in the case of acquisition of new information system services. Every aspect of the information system will have a baseline developed by the IST team through analysis of the product in a controlled environment under (SI-2) as established in the System and Information Integrity Policy. Once the security of the product is deemed safe, the baseline will be generated and reported to the IST manager who will approve/reject the baseline configurations depending on the functionality and necessity of the information system.
   1. Baseline configuration is not determined only by the default state of the product when installed or received from a vendor. Though a baseline will be generated for that, the primary baseline is created for the product once it is updated and integrated appropriately and serving a function within the information system.
   2. Baseline configuration will be maintained and updated as new updates or products are implemented or installed as new baselines must be created as the information system changes over time. Aside from changes from the occasional updates, the information system will be under review annually to determine if new baselines will need to be established or not.
2. Configuration Change Control (CM-3): PCT’s IST manager will be given the responsibility of configuration management, so all configuration change controls must be reported to him/her. Changes to the information system may be reported as a documentation by the IST team or other positions that work with the information system. The IST manager would then determine if the change is configuration-controlled and make a decision to further analyze the possible change or discard the idea. If the proposed configuration-controlled change is approved, it would have to run through control 3, (CM-4). Documentation will be produced for the change’s entirety and SDLC components as necessary. Once all analysis is done, a report will be generated for the IST manager to approve the change or discard it.
   1. Records of configuration-controlled changes to the information system will be retained for a minimum of 3 years. This includes records of audits and reviews of activities associated with the configuration-controlled changes.
3. Security Impact Analysis (CM-4): PCT’s IST team and manager will be responsible for conducting analysis of the information system before changes to determine possible security impacts. The analysis will be done in a controlled environment under (SI-2) as established in the System and Information Integrity Policy. Analysis of the original product and baseline will be included as well as possible outcomes of changes. All methods done in the controlled environment will be documented and a final report and solution will be made and delivered to the IST manager for further actions to be made.
4. Access Restrictions for Change (CM-5): PCT’s IST manager will produce a defined document outlining the enforcement of physical and logical access restrictions that deal with the information system. Only the IST manager as well as select positions are given physical access through key cards to enter the vicinity where changes to the information system can be made. Furthermore, special login credentials are required to access the information system as well as proper authorization and authentication to make any changes.
5. Configuration Settings (CM-6): PCT’s IST team and manager will be assigned the task of establishing documents for configuration settings for information technology products used in the information system including but not limited to: servers, network components, operating systems, and applications. The IST team and manager will determine a set parameter for changes that can be made to hardware, software, or firmware components for the information system based from the baseline from control 2. The configuration settings will be implemented once approved by the IST manager. The information system will be monitored for any anomalies and deviations from the established configuration settings. If one is discovered, then it must be identified and documented and reported to the IST manager in the case it holds a threat against the information system.
6. Least Functionality (CM-7): PCT’s IST team and manager will be responsible in determining the capabilities of the information system as well as disabling all unnecessary functions, ports, protocols, and services. Single function information systems will be implemented so as not to overload a single information system. These can include but is not limited to email servers, web servers, FTP server, and Telnet servers. Certain ports for certain servers must be disabled as it is unnecessary. Example being but not limited to an email server requiring port 25 (Simple Mail Transfer Protocol). Once required ports are deemed necessary by the IST manager and PCT’s network administrator, then other ports that are unnecessary can be disabled. Nonsecure
   1. A review will be done on each individual information system annually or when a change is implemented to identify any unnecessary or unsecure functions, ports, protocols, and services. If identified, they will be disabled as well as a documentation and report of what was done.
7. Information System Component Inventory (CM-8): PCT’s IST team and manager will be tasked with developing and documenting an inventory of the information system components that describes the current information system as well as its functions and components that are within authorization boundary of the information system. The level of granularity will be determined by the IST manager necessary for reporting purposes. The information system component inventory will be scheduled for review annually unless updated, which will require a review to be created then.
8. Configuration Management Plan (CM-9): PCT’s IST team and manager will be responsible for developing, documenting, and implementing a configuration management plan for the information system. The plan will address roles, responsibilities, and configuration management processes and procedures. Configuration will be taken into account as an implementation of security throughout the system development life cycle (SDLC) and as outlined in (SA-3) under the System and Services Acquisition policy. The plan will define configuration items as established by the IST manager and team. The plan will be protected from unauthorized disclosure and modification.
9. Software Usage Restrictions (CM-10): PCT’s IST team will monitor the appropriate use of software as agreed upon during the purchase of a license/contract as well as copyright laws. Software will be distributed properly by quantity as outlined in the license as well as being tracked to ensure the contract is being upheld.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to he information system starting from its inception until it is resolved. Documentation of he exception must be made and may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. In the occurrence of an exception, the IST manager will be granted the ability to make decisions to the information system that may break policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or until the issue is resolved. Exceptions will remain active until the college executives deem that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the ‘Human Resources Management Policy.’

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

IST – Information Systems and Technology

Revision History:

05/07/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Information System

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain a Contingency Planning (CP) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. The policy help aid in establishing processes to be taken in the case of the issues with information system including corruption that may result in the exposure of confidentiality, integrity, and availability of the information system. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to ensure the availability and further confidentiality and integrity of PCT’s information system infrastructure, hardware, and software; creating a process for them to operate on in the case of an emergency that leaves the information system inoperable on PCT’s main campus. Security measures and operation of the information system is the goal of this policy in the case of a disaster. PCT will continuously be improving the security of the information system to protect it from adversaries that could cause it to be unavailable through additional security measures and best practices through training. The policy mostly addresses the continuity of the information system and operations around the information system in the case of a disaster.

Audience:

This policy will primarily be for, but not limited to, the information technology staff on PCT campuses, executives for mission critical decisions, and the legal team in the case of legal issues.

Policy:

Each campus under PCT must comply and follow a formal, documented program that outlines the necessary steps to take in the case of an incident involving the information system that causes it to be unavailable whether it is through the down state of firmware, software, or hardware. The document will provide methods of training to staff members to follow proper procedures in the case of a disaster with the information system.

The program will annually asses the information system to determine whether the controls and guidelines are adequate and being met. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The establishment of information system back to a secure and available state will be maintained through a developed contingency plan, alternate sites for storage and processing, as well as multiple telecommunication services as backups in case the main provider becomes unavailable.

The following controls are college-wide and to be implemented, in use, and in continuous improvement. They are derived from the CP controls described in the NIST SP 800-53 (Rev. 4). Each campus under PCT must establish and maintain the following controls:

1. Contingency Plan (CP-2): PCT’s IST team and manager will work alongside the contingency team and incident response team to develop, implement, and maintain a contingency plan suited for the continuity of the information system in the case of a disaster. The contingency plan will consist of, but not be limited to:
   1. The identification of mission critical business functions of PCT. These consist of email servers as the student and faculty body highly rely on the use of email as a means of communication. Website server as many main functions of PCT is done through not their public website, but their website for students and faculty, being ‘mypct.pct.edu’. Additional issues consist of the loss of communication through telecommunications or the loss of connection to the Internet on PCT campuses.
   2. Recovery of the information system would be to bring it back up to a running state that is able to provide the basic functions of communication, as additional features can be brought up after a means of communication is established. Additionally, the IST team must comply to the contingency plan as laid out by the IST manager, contingency plan team, and college executives. Contact information should be available to all IT staff members that work in direct or around the information system.
   3. On top of the essential requirement of establishing communications above all, we need to restore the information system back to its original state, or as close as possible to its last functioning state. However, during the time, since mission critical functions are met, the IST, contingency, and incident response team will be analyzing and aiming to pinpoint the cause of the disaster and if it is linked with firmware, software, or hardware. If it is a firmware, software, or hardware issue, then that specific product or service will either have to be updated or terminated from use.
   4. All final decisions on the contingency plan must be approved by the IST manager as well as the college executives before any training or copies are to be administered or distributed.

Once the contingency plan is approved, copies of the procedures will be delivered to all staff members that work in direct or around the information system as well as a means of training in the case of an occurrence. The incident handling team will be part of the creation of the contingency plan as they will need to develop a proper incident response plan to match the contingency plan. The contingency plan for the information system will be under review annually and updated to address changes in the organization, information system, or the environment it operates on. Review must be done if issues are encountered during implementation/execution of the contingency plan as well. The IST manager will be the designated individual to report changes in the contingency plan to as he/she oversees the construction of the plan. The IST manager will also be the only individual with authorization to access the contingency plan, thus protecting it from unauthorized disclosure and modification.

1. Contingency Training (CP-3): PCT’s contingency plan and IST manager will be responsible for developing a contingency training program and oversee the training of staff. All staff members that work in direct or around the information system must take the contingency training course within 30 days of being hired for the position. A mandatory annual training will be done for all staff members that work in direct or around the information system. Additionally, when the information system changes and the contingency plan is redone, which would cause the training program to change, staff will need to take a training within 30 days of the new contingency plan being adopted.
2. Alternate Storage Site (CP-6): PCT has multiple campuses besides main campus. The college owns two main off-site locations that is to be used as alternate storage sites. The one being the Kathryn Wentzel Lumley Aviation Center located at the Williamsport Regional Airport located in Montoursville, PA. The other being the Herman T. Schneebeli Earth Science Center located in Montgomery, PA. Both establishments are owned and operated by PCT and will have the necessary firmware, software, and firmware to act as main campus’s information system backup storage and able to do data retrieval. As established in all PCT security policies; all campuses under PCT must follow the controls provided in every information security for every information system.
3. Alternate Processing Site (CP-7): PCT’s two off-site locations established in CP-6 will be the off-site location for processing the information system and data as well. Not only just providing a means of storage, these two sites also has the necessary equipment and supplies to ensure that mission critical operations can be provided. As established in all PCT security policies; all campuses under PCT must follow the controls provided in every information security for every information system.
4. Telecommunication Services (CP-8): PCT will have a minimum of two Internet Service Providers that operate on different networks so in the case of one not operating, the other can take its place while it is being troubleshooted. Telecommunications is one of the mission critical functions as PCT provides many of its services through the Internet which the information system is required to have to operate.
5. Information System Backup (CP-9): PCT’s information system will do regular weekly backups of new user, system, and information system security related documents involving new information. A monthly full backup will be done as well for these three information categories. The confidentiality, integrity, and availability of the backups will be protected as established in all PCT security policies; all campuses under PCT must follow the controls provided in every information security for every information system. The backups will be the off-site locations established in CP-6.
6. Information System Recovery and Reconstitution (CP-10): PCT’s IST team will be responsible to bring the information system back to a running state after the disaster occurred. The process will begin immediately as soon as conditions are deemed safe through varies methods of analysis, whether it’s a physical location issue or a firmware, software, or hardware issue. The information system will be brought up to the running state of its last backup from one of the off-site backups.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system starting from its inception all the way until it is resolved. Documentation of the exception must be made and may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may not abide by policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives and IST manager come to a conclusion that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the “Human Resources Management Policy.”

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

IST – Information Systems and Technology

Revision History:

05/07/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Information System

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain an Awareness and Training (AT) policy as outlined in the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, Revision 4. The policy will help aid in producing a training process as well as awareness system so employees can be more knowledgeable in practices to protect the information system from damages that could cause disruptions to the daily functions of the college and the confidentiality, integrity, and availability of the system. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to help ensure the confidentiality, integrity, and availability of PCT’s information system infrastructure, hardware and software; protecting it from internal and external threats. The policy will help aid in producing a training system for employees to understand requirements and procedures in securing the information system as well as an awareness process to keep employees up to date on updated procedures. Proper training is required for all employees that work in direct or around the information system and an awareness program will be developed so training materials will remain as a part of the job. Through training and awareness, we can reduce the likelihood of a disaster in the information system.

Audience:

The policy will be for all personnel that work in direct or around PCT’s information system.

Policy:

Each campus under PCT must comply and follow a formal, documented program to implement and maintain a consistent training and awareness program for the purpose of educating personnel in job responsibilities with the information system that could lead to a breach in the confidentiality, integrity, and availability of the information system.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the information system will be maintained through, but not limited to personnel required to take such training, training for specific roles, as well as a maintenance of records of training programs and personnel participation.

The following controls are college-wide and to be implemented, in use, and in continuous improvement. They are derived from the AT controls described in the NIST SP 800-53 (Rev. 4). Each campus under PCT must establish and maintain the following controls:

1. Security Awareness Training (AT-2): PCT’s IST team and manager, contingency team, and incident response team will produce a security awareness training program for all personnel working in direct and around the information system. Personnel may include contractors working with the information system, in which case, they must comply by PCT’s security standards and the security policy will apply to them as well as all others working with the information system. All new hires will have to complete the training within 30 days of being selected for the job position. Changes of the information system would require an update of the awareness training program, requiring personnel to complete the updated training within 30 days of the update. Additionally, a mandatory annual training will be required by all personnel working in direct or around the information system.
2. Role-Based Security Training (AT-3): PCT’s IST team and manager, contingency team, and incident response team will develop additional security training for specific roles interacting with the information system. One of which is the specific training for the IST manager role and each team, consisting of the IST, contingency, and incident response teams. All training time frequencies follow the exact format of (AT-2).
3. Security Training Records (AT-4): PCT’s IST team and manager will document information system security training activities for all individuals for the entirety of the individual being an employee under PCT and 5 years afterwards as defined in the “Employee Records Retention” document by human resources. Business individuals who have undergone training will have their activities documented for a minimum of 5 years.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system starting from its inception all the way until it is resolved. Documentation of the exception must be made and may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may not abide by policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives and IST manager come to a conclusion that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the “Human Resources Management Policy.”

References:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

Definitions:

Enter definitions here. Consider any words, concepts, or acronyms that are not commonly known by the audience. You don’t need to define everything.

Revision History:

05/07/19 – Policy Created and Implemented.

Implementation Date: 05/07/19 Control Area: Information System

Approval: Jeffrey Yang Review Date: 05/07/19

Objective:

The Pennsylvania College of Technology (PCT) will establish, implement, and maintain a Data Encryption (DE) policy following standards outlined in the Advanced Encryption Standard (AES) as established by the National Institute of Technology (NIST). The policy will aid in the security of data within PCT’s information system, protecting it from disruptions to the daily functions of the college and the confidentiality, integrity, and availability of the system. Unless otherwise specified, the head of the information technology department will be responsible for updating this policy annually for review and/or changes.

Purpose:

The purpose of this policy is to help ensure the confidentiality, integrity, and availability of PCT’s information system infrastructure, hardware and software; protecting it from internal and external threats. The policy will help aid in producing a procedure in the encryption of data throughout PCT’s information system. Through proper encryption methods, we can reduce the likelihood of a disaster in the information system.

Audience:

The policy will be primarily be for, but not limited to, the information technology staff on PCT campuses, executives for mission critical decisions, and the legal team in the case of legal issues.

Policy:

Each campus under PCT must comply and follow a formal, documented program to implement and maintain encryption methods and procedures throughout data on the information system with the purpose of protecting its confidentiality, integrity, and availability.

The program will annually assess the information system to determine whether the controls and guidelines are adequate and being met. If not, the ability to adjust either the guidelines or the actions will be granted so the criteria can be met. The security of the information system will be maintained through, but not limited to the encryption of resting and moving data, portable devices, and encryption key management.

The following controls are college-wide and to be implemented, in use, and in continuous improvement. The controls are aliased as DE and follows guidelines outlined in the AES as well as other necessities required of PCT’s information system. Each campus under PCT must establish and maintain the following controls:

1. Data at Rest (DE-1): PCT’s IST team will be responsible for the encryption of all firmware, software, and hardware in the information system such as but not limited to hard drives, partitions, and virtual disks. Resting data includes all backups of the information system on other campuses, such as the Kathryn Wentzel Lumley Aviation Center and the Herman T. Schneebeli Earth Science Center as outlined in CP-6 in the Contingency Planning policy. The encryption method to be used is the 256-bit encryption method as standardized by the AES.
2. Data Transmission (DE-2): User’s of PCT’s information system must oblige by the college’s acceptable use policy, through services provided such as wireless access, email, or other methods of communication provided through the information system. The IST team will be responsible for ensuring the encryption of transmission of confidential data such as Personal Identifiable Information (PII). This policy affects all vendors, customers, or entities that do business with PCT when transfer of confidential data over a public network such as the Internet is used. The encryption method may vary, but the use of an algorithm that uses the 256-bit encryption method as standardized by the AES will be prioritized.
3. Portable Devices (DE-3): Portable devices are methods of data-at-rest, but can be incorporated in practice of data transmissions. Not limited to, but example being the use of USB devices. Though confidential data should not be stored through portable devices, cases may arise where it is necessary, such as if the information system’s wireless communication is down, so services such as SSH cannot be used. Portable devices such as USB devices may be necessary. In this case, encryption of the portable device is mandatory. Other portable devices include cellphones, laptops, tablets, or other personal digital assistants (PDA). Employees of PCT that work in direct or around the information system is prohibited from carrying confidential data on their PDAs. Encryption methods should still be incorporated on these devices for best practices.
4. Encryption Key Management (DE-4): PCT’s IST manager will be responsible for encryption key management, as well as a senior staff of the IST team. This method provides a separation of duty so the IST manager does not have total control over the creation and distribution of the keys. The IST manager will be given access to view the keys and verify encryption of files and backups. The IST senior member will be responsible for the functions of the encryption key. Additionally, credentials to the encryption keys will be securely stored and given to the President of PCT in the case of emergencies. Special training will be required for these roles as outlined in AT-3 in the Awareness and Training policy.

Exceptions:

Exceptions will be made in the case of mission critical issues that can cause harm to the information system starting from its inception all the way until it is resolved. Documentation of the exception must be made and may consist of but not limited to: date of exception granted, exception granted personnel, who granted the exception, brief description and purpose of the exception. If the time of an exception ever occurs, the IST manager will be given the ability to make decisions to the information system that may not abide by policy. If the IST manager is not present at the time, the college executives may appoint a temporary IST manager until the IST manager arrives or when the issue is resolved. Exceptions will remain active until the college executives and IST manager come to a conclusion that the issue is contained and everything is running as normal/expected.

Disciplinary Action:

Failure to adhere to this policy could result in the suspension or discontinuing of the information system by the information system manager at the time. Further denial to follow the policy may lead to termination of the job. These decisions will be made by PCT’s human resources department through controls outlined in the “Human Resources Management Policy.”

References:

Advanced Encryption Standard (AES)

Definitions:

IST – Information Systems and Technology

AES – Advanced Encryption Standard

Revision History:

05/07/19 – Policy Created and Implemented.