IT Security and Operational Policy

Version 1.8, November 30, 2015

1 – Information Technology Leadership

1.1 IT Roles and Responsibilities

The responsibility for Hocking College's information and information systems must be integrated into all aspects of the college's business operations and use of technology. The roles and responsibilities in this section focus only on the information security roles and responsibilities for the individuals that are involved in college's leadership of the information security and operations program. These individuals will have additional responsibilities not covered within these sections.

IT Leadership
The IT Leadership represents the CIO position and is responsible for establishing and overseeing the department-wide information security program. The leadership reviews and approves, in writing, the information security and operations policy at least annually.

Additionally, the IT Leadership reviews and approves the processes, techniques, and methodologies planned for securing and maintaining information system assets and information. This includes the responsibility for the IT Infrastructure (e.g., general support systems) that provides shared services across the college.

System Administrator
The System Administrator is responsible for implementing and maintaining technical controls that enforce operational and managerial policies through mechanisms contained in the hardware, software, or firmware components of the information system. They must maintain an environment that creates a strong technical foundation for enforcement of information system security.

IT Department Users
Users is a broad term used for all personnel that interact with information system resources either in a support function, by working directly with an information system user (i.e., faculty, students). For the purposes of this document, IT department users include all college employees and contractors, including vendors and service providers.

User's responsibilities include the following:

- Comply with information security policy and apply its principles to daily work activities.

- Enforce information security policy and ensure that faculty and students comply with information security policies and procedures.
- Assume accountability for protecting sensitive information under their control in accordance with this policy.
- Report information security incidents (e.g., virus and malicious code attacks) to the appropriate IT Leadership according to established procedures.
- Cooperate in the investigation of security incidents.

Service Providers
Service providers include vendors, contractors and entities that provide IT services, information systems, and facilities housing Hocking College information systems. Service providers are responsible for maintaining security controls that are compliant with all Hocking College's security policy and procedures.

Developers
Developers are responsible for developing, maintaining, and implementing information systems that are in compliance with Hocking College security policies and procedures.

An organizational chart for the Office of Information Technology is available on the intranet. Please refer to this document for further details on what specific functions individuals are responsible for within the department.

1.2 Acquisition and Purchasing

System and services acquisition requirements ensure that appropriate technical, administrative, physical, and personnel IT requirements will be included in all specifications for the acquisition, operation, or maintenance of Hocking College facilities, equipment, software, and related services or those operated by external providers of IT services on behalf of Hocking College.

1.) **For purchases and acquisitions which originate outside of the Office of Information Technology**, the following policy guidelines ensure all requirements have been identified:

- A department manager (i.e., Dean, Director) will need to identify or acknowledge the information technology need. This may be done through receiving a request from within their department or school. If the purchase or acquisition relates to information technology equipment, software, or related services, they must coordinate with the IT Leadership within the Office of Information Technology and seek feedback.

The feedback will allow the IT Leadership to verify whether the purchase or acquisition

meets functional requirements to maintain and protect the college's information technology operations, assets (including information), and individuals.

Once this feedback has been provided, the requestor is to follow the approval and acquisition process and requirements specific to their cost center.

2.) **For purchases and acquisitions which originate inside of the Office of Information Technology**, the following policy guidelines ensure all requirements have been identified:

The employee must provide a formal purchase or acquisition request (This may be done via email) to the IT Leadership.

Upon receiving the submitted request, the IT leadership will verify whether the purchase or acquisition meets functional requirements to maintain and protect the college's information technology operations, assets (including information), and individuals. The requestor will receive a written approval from IT Leadership.

1.3 Third Party Services

Financial systems as well as systems which contain personally identifiable information (PII) which have outsourced components either must have a Statement on Auditing Standard (SAS 70) Type 1 from the vendor on file, or clearly state in the contract language that they will adhere to the processes and standards outlined in the Hocking College security policies and procedures.

Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.
A formal contract is defined and agreed for all third-party services before work is initiated, including definition of internal control requirements, delivery of the third party's SAS-70 and acceptance of the organization's policies and procedures.
Lastly, the signed agreement and SAS-70 (where applicable) are filed within the Office of Information Technology.

1.4 Information Classification

Risk leadership is a process that allows Hocking College to balance the operational and economic costs of protective measures to protect the information systems and data that support the College's mission.

IT Leadership shall ensure that all information systems and data sources are classified based on their level of sensitivity. This classification shall distinguish systems among the following three levels: *low*, *moderate*, and *high* sensitivity.

In making this assessment, IT Leadership should take the following security and operational requirements into consideration:
- integrity
- availability
- confidentiality

As part of an sustainable risk leadership program, this process and classification should be reviewed on an annual basis for all existing systems and data sources.

Additionally, for all newly developed or acquired information systems and data sources, an information classification should be determined during the planning or acquisition phase. By classifying the system prior to development or deployment, leadership can ensure the proper security mechanisms will be put in place.

1.5 System Inventory

The Office of Information Technology shall develop and maintain an inventory of major information systems operated by or under the control of Hocking College.

This inventory will include all system interfaces.

The system inventory shall be updated as necessary and reviewed annually by IT Leadership or an appropriately assigned resource.

1.6 Individual System Security Plans (formal policy over requirement only)

IT Leadership is responsible for the security controls (i.e., safeguards or countermeasures) for an information system as part of leadership of risk and the leadership of information system security.

There may be the circumstance where a system requires additional safeguards or security configurations which are different from or not discussed within the security policy. A common example would be a system which processes credit card transactions which would have additional regulatory security requirements (i.e., PCI).

IT Leadership shall create, when appropriate and necessary, system-specific security plans for systems which may not conform to this general security policy.

NOTE: IT Leadership may also create an additional security policy for systems which share an information classification of high (see *section 1.4* for additional details on information classification).

IT Leadership shall review and update any system-specific or classification-specific security policies on an annual basis.

2 – System Development Life Cycle

The System Development Life Cycle methodology includes all of the necessary phases in regards to the development or acquisition of a system.

The Hocking College SDLC is comprised of seven phases. The phases include the initiation phase, planning phase, requirements analysis phase, design phase, development phase, testing phase and implementation phase.

This methodology is to be used in the development and acquisition of systems for Hocking College. Further, if any aspects or the project overall is being completed by a third-party, all documentation and deliverables described herein are required to be completed as part of their work.

The following will discuss the seven SDLC phases and how they must be implemented at Hocking College. The project lead has to ensure that the appropriate documentation for each phase is documented and maintained for review by IT Leadership.

2.1 Initiation Phase

The development or acquisition of a system is initiated when a college need or opportunity is identified. A Project Lead is appointed to manage the development or acquisition as a project and depending on the recipient on the system, a Project Sponsor may be committed from a related college school or department. Furthermore, a project change ticket is created for this phase of the project and assigned to the Project Lead or Sponsor. The ticket will serve as a holding place for documentation created in this phase, and allow the Project Lead or Sponsor to approve the completion of this phase, if a decision for continuation of the project is reached by IT Leadership.

The Project Lead is responsible for documenting the college need in the form of a Business Case. Ultimately, the Business Case is a formal method for describing the college's reasons for the project. The Business Case should outline the project scope, expected benefits, potential organizational changes, any budget requirements and potential technology constraints. The format of this Business Case will be provided by IT Leadership in the form of a template.

Once the Business Case is completed, the Project Lead schedules a review meeting with key IT Leadership to review the Business Case and seek approval for the project. Approval should be based on associated risk, risk requirements, cost/benefit analysis, overall cost and tangible/intangible benefits.

NOTE: IT Leadership may involve the Project Sponsor within this approval phase at their discretion.

If approval for the Business Case is denied, the project will not continue and this should be documented within the closed change ticket. However, if the Business Case is approved and capital is needed for the project, the purchasing & acquisition policy (*Section 1.2*) shall be followed to gain approval.

The project leader is responsible for ensuring the above steps have been completed before the project can begin the Planning Phase.

2.2 Planning Phase

During this phase, the Project Lead is responsible for describing and developing how the system, once implemented, will affect the college and how it is operated. The Project Lead should ensure that information security and privacy is assessed at this part of this phase.

The Project Lead is responsible for creating an overall Project Plan to ensure that the system meets the college need and is delivered on-time and within budget. Furthermore, project resources, tools, activities, schedules, and communication methods to stakeholders should be defined within the plan, if required or requested.

Depending of the scope and size of the project, a project team will be assigned and assembled during the Planning Phase. The team should strive to contain both functional and technical experts. In particular, functional experts serve as key knowledge sources for current college processes and contacts.

Note: if at any point during the SDLC the system/plan deviates from what was approved in the Initiation Phase, (i.e. scope creep, additional capital, more resources, longer development time, etc) the Project Lead must communicate this back to the Project Sponsor and or IT Leadership and gain additional approval. The approval will be documented by re-approving the project within the change ticket.

The created Project Plan and related documents are required to be maintained or referenced within the project change ticket.

The Planning Phase will be deemed completed once the Project Sponsor or IT Leadership completes a review of and approval to the Project Plan.

The project lead will ensure the above steps have been completed before the project can begin the Requirements Analysis Phase.

2.3 Requirements Analysis Phase

A Requirements Document is delivered as part of the Requirements Analysis Phase. This document includes three defined sections of requirements—general, functional and technical. Once again, this document is the responsibility of the Project Lead, although information to complete the document may come from several sources, including any members of the project team.

- Overall, the general requirements section summarizes the entire project. It provides detailed information regarding the following areas: project description, background, resources, assumptions/constraints, and interfaces to external systems. In particular, the previously defined project plan may be used to complete the project description.
- The functional requirements section describes the core functionality of the system and includes the data and functional process requirements. Requirements may be expressed using data flow diagrams, text, or any other technique or model which clearly represents the processes performed by the system. The functional requirements will clearly show how the new system will impact the operations of Hocking College.
- Lastly, the technical requirements describe the non-business characteristics of the system. Some of the key areas addressed in this section include data security, audit trails, reliability, recoverability, availability, performance, processing integrity and system capacity. In particular, providing the appropriate security design is necessary to ensure the system is only accessed by the proper

personnel. Availability is also a crucial operational requirement—a system that is not available when needed may hinder the instruction and mission of the college.

Once completed, the Requirements Document is attached within the project change ticket as documentation for the Requirements Analysis Phase. For the Design Phase to begin, The Requirements Analysis Phase will be deemed completed once an approval is provided by IT Leadership or the Project Sponsor.

2.4 Design Phase

There are numerous activities and deliverables that should be considered as part of the Design Phase. These deliverables include a Systems Design Document, Test Plan, and Implementation Plan. The creation of the previously listed documents is overseen by the Project Lead; however, the responsibility to create them may be assigned to other Project Team Members as needed.

- The Systems Design Document is the main deliverable from the Design Phase. It is created using information that is obtained in both the Planning and Requirements Analysis phases and specifically address system attributes and database design. The completed design document is then used in the Development Phase.
- In regards to plan documents, a Test Plan is created in the Design Phase. The Test Plan identifies the tasks and activities that need to be performed so that all aspects of the system, including integration, new functionality, security, and the overall system are adequately tested. In particular, the Test Plan may include testing scripts which are executed during the Testing Phase when users are testing the system.
- The Implementation Plan encompasses all activities that are carried out within the Implementation Phase. The plan describes how the system will be deployed, installed and transitioned into an operational system. The plan contains a brief description of the major tasks involved in the implementation, the overall resources needed to support the implementation effort (such as hardware, software, facilities, materials, and personnel), and any site-specific implementation requirements.
- A Conversion Plan is needed when if converting data from an existing system to a new system. This plan ensures that all data is properly transferred and tested.
- A Training Plan is also created during the Design Phase. In summary, the Training Plan outlines the objectives, needs, strategy, and curriculum to be addressed

when training users on the new or enhanced system. This material may be in the form of a Help File or FAQ. Ultimately, the complexity and scope of the system will dictate how involved the Training Plan needs to be for anticipated audience.

Once completed, all created materials are attached to the change ticket. In order to proceed to the next phase, the Project Lead or Sponsor must review and approve all of the above documents that are created.

2.5 Development Phase

The detailed specifications produced during the Design Phase are translated into hardware and executable software during this phase. In particular, the System Design Document is referenced and followed.

- If development is completed internally, System Analysts will complete the following activities: code and develop programs/assemble hardware, debug and unit test programs, develop data conversion programs, and document all system modifications. Responsibility for the above tasks will be assigned by the Project Lead.
- If development is completed externally, Functional Users and IT Leadership ne to be involved in the Development Phase. Likewise, if a system is purchased, Systems Analysts will aid in testing programs and identifying issues. They may also be responsible for reviewing or creating user documentation and training selected users for unit testing.

2.6 Testing Phase

During the Testing Phase, the various components of the system are integrated and systematically tested to ensure the system is ready to be used in production. End Users may be involved with testing the system to ensure that the functional requirements, as defined in the functional requirements document, are satisfied by the developed or modified system.

If deficiencies or problems are discovered they are recorded and tracked which should be reviewed by the project team.

- System testing includes a series of tests to ensure that everything related to the system is working properly. For this reason, software performance, response times, security, and overall system performance is tested.

- User acceptance testing is the process of ensuring that the system is production ready and satisfies all documented requirements. Again, results from the test scripts are either recorded within the test scripts or added as a supplemental to the Test Plan.

All plans (implementation, conversion, and training) created in the Design Phase and enhanced in the Development and Testing Phases are finalized prior to implementation. Once these documents are completed and finalized, they must be reviewed by IT Leadership.

The Project Lead is responsible for reviewing all documentation prior to completing the approval to enter Implementation Phase.

2.7 Implementation Phase

All plans created in the Design Phase are fully carried out in the Implementation Phase. These plans include the Implementation, Conversion and Training Plans.

- In particular, training (if required) is scheduled per the objectives defined in the Training Plan. Also, if applicable, the tasks outlined in the Conversion Plan are completed to ensure that data has been correctly transferred between environments.
- The Implementation Plan is fully rolled out based on a pre-determined schedule. After the Implementation Plan is completed, the system should be completely operational in the production environment.

Determining whether a post implementation review (PIR) is appropriate is the responsibility of IT Leadership. The overall objective of the review is to assess the adequacy of the system. A PIR review if performed would be completed upon the successful implementation of the system. The review should also evaluate the projected costs/benefits and the return on investment. Finally, any other concerns or issues related to the project, project methodology, or project leadership should be discussed so changes can be made in the future, if necessary. The final document created for the Implementation Phase is a signoff form which should be formally signed by the Project Lead, Sponsor (if applicable) and IT Leadership. This should also be attached to the change ticket assigned to the project.

All subsequent changes to the system will be handled per the change leadership process discussed in *section 3* of this policy.

3 – Change Leadership

3.1 Change Leadership Policy

3.1.1 Roles

The Change Requester, Change Analyst, IT Leadership and Business Process Owner have unique roles within the change leadership process. They are all responsible for overseeing changes within the IT infrastructure and ensuring that documented change procedures are followed.

Change Requester – Any Hocking College IT user, including but not limited to faculty who submit a change request through the ticketing system.

Change Analyst – The Change Analyst is the person who designs, executes and documents changes. Ultimately, this is the person who resolves the ticket whether it is categorized as a High Priority, Normal Priority, Low Priority or Emergency Priority change. The Change Analyst may be assigned by IT Leadership. For unassigned Low and Emergency Changes, anyone in the Office of Information Technology group may assign the request to themselves. Ultimately, the Change Analyst is responsible for the following:

- Follow applicable standards.
- Document changes according to the standards for the tools being used.
- Ensure training (when appropriate) and communication of change to the end user occurs.
- Oversee the execution of the implementation.
- Ensure that appropriate testing has been accomplished and approvals obtained before implementing changes to production.

IT Leadership – The IT Leadership is responsible for ensuring the change leadership policy and processes are followed by Change Analysts.

Business Process Owner – A Business Process Owner (BPO) is an individual within the department or school related to the change request. They can be thought of as the intended audience of the change.

The BPO may provide comments before, during and after implementation of a change. This may include documenting that the tests were run successfully and no

undesirable side effects were experienced.

3.1.2 Types of Change

All changes fall into one of four priorities of change: High Priority, Normal Priority, Low Priority, and Emergency Change. These priorities should also reference the perceived impact or risk of the change to the Hocking IT infrastructure and drive the process steps which must be followed and the approvals that must be given. The priorities of changes are listed in order from highest to lowest priority, (with the exception of Emergency Change) and are given a formal definition.

High & Normal Priority/Impact Changes

Both Normal and High Priority/Impact Changes assume a medium-to-high level of risk. Additional criteria for classifying changes as High/Normal Priority are listed below.

- Financial-related production data or system.
- Changes to data or systems involving PII information (student and/or faculty).
- Implementation requires a service interruption outside of regularly scheduled downtimes.
- New project implementations where scope included detailed SDLC methodology (see requirements in *section 2*)

Low Priority/Impact Changes

A Low Priority/Impact Change is characterized by its low risk. These changes carry low functional and technical risk and affect a small group or individual users. These types of change may have been pre-approved by the Helpdesk. The following are examples of a Minor Change:

- Changes to existing functional reports.
- Move a phone.
- Replace a monitor.

Emergency Change

This type of change is used to fix critical problems in existing functionality in order to restore service. It requires an incident logged in the ticketing system, and completion of required approvals within 3 business days. The IT Leadership reviews all emergency changes for appropriateness.

3.1.3 Change Leadership Process

The Change Leadership process differs slightly depending on if the change is classified as a High, Normal or Low priority and also if the change is an Emergency. The following section will review each phase of the process in detail from Identification & Classification to Resolution as it relates to all four priorities of change.

For purposes of this document, a *change* is defined as an action that results in a new system, service or configuration impacting one or more aspects of the IT infrastructure. Areas of impact may include hardware, communications equipment, software, application, environment, system, desktop build or associated documentation.

Identification & Classification

Any change that meets the criteria for a change (per the definition) must have a related ticket which is being used as the central change leadership system for Hocking College. A request can come from any Hocking College employee or IT user.

Since the ticketing system is being used to handle and manage all changes, a request must first be entered into the system. Requests are often entered into the system by one of three methods:

1.)A Hocking College faculty or staff member will fill in an online support request form (available via the intranet). This form will then be routed to the Helpdesk and/or department of the associated Help Topic area.

2.) Employee or IT user will call or email the IT Helpdesk and then make the change request. The Helpdesk will create the ticket and determine the appropriate priority and IT department.

3.) A member of the Office of Information Technology can create a change-related request related to an existing system or new project. After the creation of the formal ticket, the IT team member will assign the request an appropriate priority.

Review Approval – Planning

IT Leadership has access to view all change requests within the ticketing system and will informally monitor the system for all change requests that are unassigned (no Change Analyst). Additionally, all Normal or High Priority changes will require the approval of IT Leadership before any work can begin on the change.

For all Low priority changes, the Helpdesk or any IT team member can self-assign the change request and begin work on the change.

IT Leadership should also review any Emergency Changes after resolution to ensure the activities completed as part of the change are documented.

Work in Progress – WIP

The WIP phase represents the greatest amount of time spent in regards to the Change Leadership Process. The Change Analyst is responsible for completing this phase. Once again, what occurs in this phase is dictated by the type of change.

Normal or High Priority/Impact Changes

- All important information related to the change is added to the comments section of the associated ticket.

- IT Leadership may assign someone else to complete testing requirements or implement the change into production.

- IT personnel shall ensure that the general comments section of the ticket along with any related email communications includes no confidential, PII privacy, or password information.

Low Priority/Impact Changes

- All important information related to the Low Priority Changes is added to the comments section of the ticket.
- Although not documented, all Low Priority Changes may be informally tested by the Change Analyst prior to being implemented in the production environment.

- IT personnel shall ensure that the general comments section of the ticket along with any related email communications includes no confidential, PII privacy, or password information.

Emergency Change

- All important information related to the Emergency is added to the comments section of the ticket.

- Approval is obtained after service has been restored.

- IT personnel shall ensure that the general comments section of the ticket along with any related email communications includes no confidential, PII privacy, or password information.

Note: Testing should be completed on all High/Normal Priority and Emergency Changes. Informal testing is optional but recommended for Low Priority Changes when applicable.

Implementation / Resolution
All changes are implemented as a part of the final phase. In the case that training is required, training should occur prior to implementation.
Once changes have been implemented in production the change request status is changed by the change analyst to 'closed'.

3.1.4 Segregation of Duties

As part of a best practice, when making any changes to financial-related systems the change analyst should ensure there is appropriate segregation of duties. The change analyst (Developer) should not be the resource responsible for implementing their own code changes into production.

If there are no other appropriate resources available to migrate the change, the change analyst should provide notification to IT Leadership and seek a special approval. If this circumstance occurs, additional detailed documentation should be added to the change ticket.

As a reminder, if the change is classified as Emergency priority, the primary objective is for service restoration. This should be taken as the primary consideration and additional documentation may be provided within the ticket.

4 – Computer Operations

4.1 Business Continuity Plan

NOTE: This italicised sections of the Information Security & Operations Policy is currently being developed and under review.
The objective of business continuity planning is to ensure the continuity of Hocking College's instruction and missions in the event of unanticipated computer processing disruptions such as operational failures or site disasters that destroy or prevent access to the computer equipment, data, and software on the Hocking Campus.

Key stakeholders and departments:

Executive Leadership: President, VP Financial Services, VP Administrative Services, VP/Provost, CIO
IT staff: System Administrator, Network Administrator, Colleague Administrator, CIO
Student Services: Director of Enrollment Services,
Academic Support: Director of Academic Scheduling,
Cashiers and Records: Bursar, Payroll Manager, Controller

Mission critical applications:

Colleague, webadvisor, webui, network services

Mission critical buildings and/or rooms:

Shaw labs, JL 175, Campus Safety, cashier and records

In the case of a power outage on campus, cashiers and records will be designated as a generator supplied hot spot for mission critical business operations.

To help ensure high availability a generator will be used on all mission critical buildings and/or rooms identified within this plan.

Disaster Recovery Plan

Every 6 months the key stakeholders identified on this plan will execute a test of the disaster recovery plan.

Detailed plans can be found in the Business Continuity Planning Document.

Hocking College IT staff along with designated power users will perform

4.2 Physical Security

Hocking College's primary data center entrance is equipped with a biometric finger print reader with a keypad and isolated key. Access to the computer room area is restricted to the technical services personnel who are responsible for operations of the equipment as well as campus safety and the locksmith.

All access to the IT data center and other computer rooms must be authorized by IT Leadership.

Additional computer rooms are protected via traditional lock & key. Access is limited to facilities leadership and personnel within the Office of Information Technology.

The computer room access reviewed and signed by IT Leadership on an annual basis.

4.3 Environment Security

Hocking College's data center is equipped with separate air conditioning units, temperature sensors, water-based fire suppression system, appropriate UPS systems and a generator.

Periodic maintenance and tests are performed and recorded to ensure these units are functioning normally.

4.4 Job Scheduling

Job Scheduling is the responsibility of the system administrators. This responsibility includes the creation of new job entries or making revision to existing.

Requests for changes or additions to job schedules for a material financial system (which includes the DBMS) and its supporting infrastructure are handled as change tickets. Tickets for job scheduling will improve the change leadership structure related to this critical system.

4.5 Data Backup & Recovery

Backups of systems and their data are taken daily or as deemed appropriate by IT Leadership. The data backup requirements should take into consideration the system's information classification (defined in *section 1.4* of this policy)

Distributed Systems

On the midrange servers, two types of backups are taken. All system and data file changes are backed up differentially. Additionally, a full system backup is taken based on an appropriate schedule.

Backups are automatically scheduled within the midrange server backup software and logging of these backup jobs is review as part of operational responsibilities of the system administrators.

In the event of a severe error, the server administration group should create a ticket to

track the incident resolution.

5.5.1 Media Protection

Backup tapes should be securely stored in a separate building on the Hocking Campus from the systems which are backed up.

Backup tapes are rotated and stored off-site in a secure safety deposit box. User access is initiated by the Office of Information Technology in conjunction with designated safety deposit box authorized officials.

Access to tape backups should be restricted to personnel within the Office of Information Technology.

Dell Vmware Environment

On the Dell Vmware cluster, Vmware guests, differential backups are taken Monday through Thursday and written to disk. Full backups are taken and stored to disk every Friday night. Live database, Full backups are taken Tuesday through Saturday and written to disk. Non-ERP system databases, differential backups are taken Tuesday through Friday. Full backups are taken Tuesday through Saturday.

Production Colleague database (SQL) is set to full recovery mode. Database keeps transactional logs in case of database corruption

Non-production environment is set to simple recovery mode.
Once a month, test restores are performed using sample files from within the Ellucian cluster to confirm backup operations are completed and verified. As part of that process we also test restore sample databases from within our production DBs. Full production DBs restores are performed nightly. The process backups the data from the production DB and performs a complete restore into the reporting environment.

4.6 Disaster Recovery

Refer to Business Continuity Planning Document

4.7 Incident Response / Handling

The Helpdesk provides a centralized process for improved communications between the Office of Information Technology and its users. It is a focal point for the communication and reporting of incidents, changes and requests.

Helpdesk records the majority of communication and activities within the ticketing system. The ticket system provides IT with an integrated approach for the submitting, distributing, tracking, managing, prioritizing, and review of the services.

Additionally, other IT departments will have support roles involving system interruptions, incidents and problems associated with their systems and job responsibilities.

Responsibility
Helpdesk Support responsibilities include the following:

Record and Classify

- Record, in ticketing system, all requests for service in IT with the initial classification of the request as an incident, question, request, or change request.
- If the request is a change, then the request needs initial classification as to the type of request. (See change request types in section *3: change leadership*).
- The Helpdesk records all pertinent information into the ticket, including all the required fields and as much as possible information with regards to the user's request.
- The Helpdesk provides users with the status of their service requests when they call or email inquiring the status of their ticket.

Monitor

1. The Helpdesk monitors incidents to detect problems (multiple incidents with the same root cause). An example of this would be a virus or worm spreading across the college network.

5 – Security Administration

Only authorized persons are permitted to access the information on the Hocking College systems. Once entrusted with a user id, a faculty member, employee or student is responsible for all operations that are performed with their user id. System or Data owners are responsible for the information being accessible only to authorized persons. All requests for access are controlled and documented.

Confidentiality and data integrity are protected by restricting the access to only those users, who need the information or are responsible for it. Giving only the needed rights to each person reduces the need to take other measures. Availability is protected by restricting access only to authorized persons who have the rights, training and skills to make appropriate changes in the system.

5.1 User Access Leadership

Every user must possess a user ID of his/her own and, in connection with it, a controlled use of the password. The only accepted exceptions are workstations which are used to perform a certain defined operation. An example can be the workstation within a computer lab. This type of user ID must not work from other locations.

User rights are documented within the ticketing system including user registration request, change and deletion in/from the systems. Documentation of all access within the ticket system allows for Helpdesk personnel to quickly access a history of all access provisioning activities.

NOTE: Ensure that no confidential, privacy, or password information is included within the general comments section of the ticketing system along with any related email communications.

5.1.1 Responsibilities: User, Manager, Helpdesk

User Responsibilities

1. The user is allowed to use only those systems which he/she has the right to use. This also means that the user is allowed to change only his/her personal settings.
2. Temporary workers, contract employees and summer workers are allowed to use only the user IDs created for them. Contract employees will be provided with a copy of the Acceptable Use Policy upon issuance of a user account for

review and acceptance.

3. The user keeps his/her personal password to himself/herself, and he/she is not allowed to share it with others.

4. If the user suspects that the password has come to an unauthorized person's knowledge, the user must immediately change his/her password, or have it changed.
5. All Hocking College faculty and employees are expected to review the Acceptable Use Policy upon start of employment.

Manager's Responsibilities

1. Managers are responsible for ensuring their employee's have the appropriate level of access to perform their specific job functions.

See *section 5.5* for additional account monitoring activities performed by Leadership.

Helpdesk Responsibilities

1. Helpdesk keeps a record of all the users of information systems and user rights via the ticketing system. Once a ticket for security access is received and approved (if required), a user id is created, appropriate access is granted and notification is sent to the requester of the ticket.
2. Removing terminated employees: When an employee is in the Termination report sent by Human Resources to Office of Information Technology, their computer accounts are immediately disabled. The accounts are deleted a week later, unless otherwise requested by leadership.

5.2 Password Leadership

Every user has a unique user ID and password. The use of unique user IDs enables all activities in the systems to be traced back to individual users. Passwords restrict access to information. The password is the user's key to information and must therefore be kept secret. Not changing passwords regularly and allowing sharing of passwords can lead to unauthorized access of the college's information systems.

5.2.1 Parameters

Below are the standard minimum password requirements for all information technology systems and environments (**if technologically feasible**). Other systems may require stricter password and account requirements (ex. Credit card processing applications). In these circumstances, the additional password parameters are defined within the System Security Plan (refer to *section 1.6*).

Campus employees are notified every 180 days about changing passwords. The passwords must be at least 8 characters in length. Suggest not using the last 4 passwords.

5.2.2 Session Termination

NOTE: This italicised section of the Information Security & Operations Policy is currently being developed and under review.

Automatic Account Lockouts occur after 10 consecutive unsuccessful password attempts. Lockout duration lasts 30 minutes.

Online resources that directly interface with the student information system (Webadvisor, WebUI, Self-Service, etc) automatically timeout after 30 minutes of inactivity.

Workstations which are part of the Active Directory are required to have a session timeout after 30 minutes of inactivity. This will assist in protecting systems and their information assets from being inappropriately accessed when users are not present.

This policy is required to be set at the Active Directory level via the GPO (AD Group Policy).

5.2.3 Password Resets

If a password reset is required, the user may contact The Computer Helpdesk by telephone or in person. Users may request password resets for multiple systems including but not limited to Gmail, Moodle, Active Directory, etc.

A user's credentials may not be communicated to any other individual including parents and spouses. For more information on FERPA guidelines please visit http://familypolicy.ed.gov/faq-page?src=ferpa-p#t30n225.

NOTE: Ensure that no confidential, privacy, or password information is included within the general comments section of the ticketing system along with any related email communications.

Positive user identification is required for a password reset.

1. In person with a photo ID
2. By telephone, providing the caller's first and last name and at least three of the following verifiable criteria:
    - Student ID/Colleague ID number
    - Last four digits of the user's Social Security Number or SEVIS number
    - Street Address
    - Birth date

5.3 Critical Business Application Access Leadership

For systems which are have been classified as high in regards to information privacy (refer to *section 1.4*) or deemed important to Hocking College, additional access management and security measures should be assessed, designed, and documented by Leadership within System-Specific Security Plans (refer to *section 1.6*).

Furthermore, access to these systems may require stricter requirements and approvals prior to the provisioning of accounts.

All systems which have modified access leadership procedures in place should have their security plans and access leadership policies reviewed on an annual basis. Additionally, all user access to these systems is required to be reviewed on an annual basis either by IT Leadership or the System Owner.

5.4 Administrator Access Control

Control of administrator access follows the same principles as the user access control. However, administrator's privileges mean that the possibilities for change and damage are much greater than for a general user. Therefore special requirements must be followed:

1. Special care must be exercised when forming a password. For example, utilizing numbers, letters and special characters as part of the password if the system allows it.
2. Administrator ID can be granted to an outsider only with the permission of the IT Leadership or a person authorized by him/her.
3. It must be checked that any delivered system neither includes default user IDs or passwords.
4. IT Leadership is required to review all administrative accounts on an annual basis to

ensure they remain consistent with the IT Leadership's intentions.

5.4.1 Least Privilege

Administrator Rights should only be granted to user's whose job responsibility requires it. Further, based on the concept of least privilege, these administrative rights should be restricted to only the access required by their job.

An example would be an IT resource responsible for backup and recovery. Their access should be restricted to programs and job schedulers as part of their job, but not necessarily DBA privileges.

5.5 Monitoring Access Control

5.5.1 Access Reviews

Based on the information classification (medium or high) of all systems and applications, and also under the discretion of IT Leadership; system access reviews should be performed on an annual basis.

A ticket should be created for all access reviews to formally document their process and completion.

IT Leadership will work with Hocking faculty and staff to determine the appropriate Hocking College resources responsible for the review. If the review is over accounting software, it may be the Finance Manager or equivalent that should perform the review.

Upon completion of the review, a formal signoff is required. This signoff should be documented within the related ticket.

6. Logical Security

6.1 Remote Access

The primary method for remote access to the Hocking College network is via VPN. VPN logon requires the proper domain security and access.

The VPN is then used to gain access to the Hocking College network over an encrypted Ipsec tunnel.

Remote access is restricted to only Hocking College employees who require it. Requests and approvals for VPN access are handled per the policy defined within User Access Leadership (refer to *section 5.1* of this policy).

6.2 Virus Protection

Virus protection for all Windows server systems and college-owned systems is required. Virus protection software installations are performed by the Office of Information Technology.

Daily monitoring of virus alerts and outbreaks are performed by the IT Leadership as part of its ongoing support.

Virus protection updates are retrieved autonomously from a centralized orchestrator server maintained by Hocking College.

6.3 Continuous Monitoring / Logging

IT System Administrators are responsible for monitoring system and security event logs. This should be completed as part of their operational responsibilities. Logs will allow system administrators to identify inappropriate or unusual activity, allow them to investigate suspicious events and research suspected violations.

Should an event be identified which will be further investigated, the following process shall be followed: The system administrator should open a ticket. This ticket will be the formal tracking and documentation method which allows historical tracking and archiving.

Acronyms

CIO	Chief Information Officer
CTO	Chief Technology Officer
DBMS	Database Management System
IT	Information Technology
PCI	Payment Card Industry security standards
PII	Personally Identifiable Information
PIR	Post Implementation Review
SAS70	Statement of Auditing Standard 70
SDLC	System Development Life Cycle
SOD	Segregation of Duties
GPO	Group Policy Object (GPO)

Definitions

PCI	Security standards were established for handling online financial transactions.
System Development Life Cycle	Guidance, policies, and procedures for developing systems throughout their life cycle, including requirements, design, implementation, testing, deployment, operations, and maintenance.
Segregation of Duties	The basic idea underlying SOD is that no employee or group of employees should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties.
Group Policy Object	A GPO is a collection of settings that define what a system will look like and how it will behave for a defined group of users.
Least Privilege	A basic principle in information security that holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions.

Frequently Asked Questions (FAQ)

What if I have a question about this policy?

Please reach out to an appropriate IT contact (refer to IT Org Chart) and he will address any questions or concerns you have.

I believe I have recommendation or update for this policy, how can this be considered for incorporation within the policy?

The department IT Security and Operational policy is a living document. It will be reviewed on an annual basis at a minimum, and more frequently as required. If you have feedback or suggestions, please provide them in an email to the appropriate IT Leadership contact.