F.51 Information Security Policy

Date
1/25
Overview

This document outlines the University of Southern Indiana's (USI) information security requirements for all employees. It is USI's policy to provide a security framework that will protect information assets from unauthorized access, loss or damage, or alteration while maintaining the university academic culture. USI management is committed to these security policies to protect information utilized by USI in achieving its mission.

Scope

All employees, contractors, vendors and third-parties that use, maintain or handle USI information assets must follow this policy. This policy includes governance of hardware, software, data, facilities, and information systems including paper media. Policy exceptions will be permitted only if approved in advance and in writing by the Chief Information Officer (CIO) and are reviewed annually.

Roles and Responsibilities

All Users

Each user of USI computing and information resources must realize the fundamental importance of information resources and recognize their responsibility for the safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems. The following are specific responsibilities of all USI information system users:

- Embracing the "Security is everyone's responsibility" philosophy to assist USI in meeting its strategic direction. This is a community responsibility to protect all our data. *Remember this data includes your personal information too.*
- Maintaining awareness of the contents of the information security policies and adhere to specific system usage, data handling, and storage requirements.
- Upon hire and at least annually, reading and acknowledgement of the USI Information Security and Data Communication and Computer Use policy.
- Completion of annual information security awareness training.
- Classifying confidential and sensitive information that is received, according to the Data Classification Policy. Limiting the distribution of this information accordingly.
- Understanding the consequences of their actions with regard to computing security practices and acting accordingly.

Human Resources

Due to their direct and constant relationship with existing employees, as well as their unique position of having the first and last interactions with new/terminated employees, the Human Resources Department has an important role with regard to USI information security. The following items are the ongoing responsibility of the Human Resources Department:

- Assisting IT Security with publishing and disseminating USI information security policies and acceptable use guidance to all relevant system users.
- Performing background checks on potential employees based on role and access to sensitive data. When possible and within the constraints of local laws, background checks should include: previous employment history, criminal record, credit history, and reference checks.
- Working with IT Security on disseminating security awareness information to system users utilizing multiple methods of communicating awareness and educating employees (e.g. posters, letters, memos, web based training, meetings, promotions, etc.).

- Working with IT Security to administer sanctions and disciplinary action relative to violations of Information Security Policy.
- Notifying IT Security when any employee is terminated.

Executive Administration

Due to their leadership requirements vice presidents, provosts, and other individuals with delegated executive authority have an important role with regard to USI information security. The following items are their ongoing responsibility:

- Assessing risks, compliance obligations, budgets, and financial costs associated with University information security and privacy, including information security and privacy incidents and information security breaches within their area of responsibility.
- Following the direction of the CIO and/or Security Team in connection with an information security and privacy incident investigation, and direct others to do so.
- Escalating Information Security policy exception requests to the CIO.
- Escalating Information Security policy violations to the CIO.

Directors/Deans/Chairs

Due to their direct reporting relationship with their department employees, directors/deans have an important role with regard to USI information security. The following items are their ongoing responsibility:

- Carrying out the USI information security culture including the importance of training and awareness.
- Establishing operating procedures and guidelines needed to comply with USI's Information Security Policy.
- Escalating Information Security policy exception requests to the CIO. (Chairs escalate to Deans)
- Escalating Information Security policy violations to the CIO. (Chairs escalate to Deans)

Information Technology

The CIO is responsible for coordinating and overseeing compliance with policies and procedures regarding the confidentiality, integrity and security of University information assets.

The Chief Information Security Officer (CISO) works with IT staff and end users to develop security policies, standards and procedures to help protect the information assets of USI. This role is dedicated to developing, implementing, and overseeing the IT security policy and framework, and providing education and awareness.

Specific responsibilities include:

- Creating new information security policies and procedures when needs arise. Maintaining and updating existing information security policies and procedures. Reviewing the policy on an annual basis and assisting management with the approval process.
- Acting as a central coordinating department for implementation of the Information Security Policies.
- Verifying that employees attend a security awareness training upon hire and at least annually.
- Coordinating annual information security risk assessment to identify threats and vulnerabilities.
- Ensuring logical and physical access controls are implemented and access to restricted areas and confidential data is monitored.
- Ensuring security alerts are monitored, analyzed and information distributed to appropriate information security, technical and end user management.
- Ensuring computer and network event logs (hereinafter referred to as logs) are reviewed and followed up on any exceptions identified.
- Creating, maintaining, and distributing incident response and escalation procedures.
- Managing Red Flags program oversight, including third party review and annual risk assessment reporting.

USI System and Network Administrators are the direct link between information security policies and the network, systems and data. System and Network Administrator responsibilities include:

- Applying USI information security policies and procedures as applicable to all information assets.
- Administering user account and authentication management.
- Assisting IT Security with monitoring and controlling all access to USI data.
- Restricting access to publicly accessible network jacks, wireless access points, gateways and handheld devices.
- Vulnerability management including routine scanning and patching

Policy

Data Classification

All data stored and accessed on USI information systems, whether managed by employees or by a third party, must follow this policy. Data stored on USI computing resources must be assigned a classification level. This level is used to determine user access, data storage and protection, data handling, data retention and destruction. Data classification is defined in four categories. In the absence of being formally classified, institutional data should be treated as *Internal Use* by default:

Listed from most sensitive to least sensitive

- Critical – Sensitive data that could result in criminal or civil penalties if exposed. Applies to the most sensitive business information which is only intended for selective access within USI.
    - Examples include passwords, encryption keys, cardholder data, bank account information, financial data, employee personnel file data, patient data (health and dental), human research subject data, and government export control restricted data.
- Restricted – Data that due to the legal, ethical, or other constraints specific authorization is required to access. Unauthorized disclosure could seriously and adversely impact the University, its employees, or students.
    - Examples include student academic data, grades, transcripts, class schedule, advising notes, and detailed environmental and control system designs.
- Internal Use - Applies to information which is intended for use within USI. Unauthorized disclosure could negatively impact the University and/or its employees. Access restrictions should be applied accordingly.
    - Examples include university owned intellectual property, policy and procedures, performance metrics, and administrative or academic data files that do not contain data that is classified as Critical or Restricted.
- Public - Applies to all other information which does not clearly fit into any of the above classifications. Unauthorized disclosure isn't expected to negatively impact the University.
    - Examples include student name, major, degree, campus map, and emergency phones.

Any public records access requests must be coordinated through Government and Legal Affairs.

IT Security Change Control

IT security change control is the formal process for making changes to IT systems that impact the existing security configuration, such as changes to the perimeter firewall, router rules, changes to server firewall rules and access control, changes to security monitoring systems, and introduction of new systems and applications into the environment. All changes are tracked and reported to IT management. Change control documentation includes:

- Impact Documentation – the impact of the change including all affected parties (internal or external), and plan for any processing change. In particular, all the systems, users and resources affected by the change and the criticality of the change rated as high, medium or low.
- Back out Procedures – if the change does not go as intended, the documented plan in place that describes the process of reverting the environment to its original configuration.
- Test Plan - set of planned tests developed to verify that the change accomplished what it was supposed to do, and does not adversely affect other system components or create a weakness in the security posture of the environment.
- Management Approval – all changes include management approval.
- Post implementation – update server and network documentation.

Data Retention

Electronic or hardcopy media are to be physically retained, stored or archived only within secure USI office environments, or offsite secured records management facilities. Data, regardless of storage location, is retained only as long as required for legal, regulatory (including federal, state, and professional), accreditation and university requirements. The specific retention length is managed by the data creator or department. Each department is responsible for establishing appropriate records management practices. The following is a guideline maximum length of record retention time:

- Student/Academic: Permanent
- Student Financial Data: 3-6 years
- Employment Related After Termination: 5 - 7 years
- Environmental Health and Safety: 3-5 years
- University Financial Records: 7 years
- Internal Use: 2 years
- Public: 2 years
- Backup Data: 1 year

Data Disposal

When no longer needed for legal, regulatory (including federal, state, and professional), or business requirements, data must be removed from USI systems using an approved method:

- Storage containers used for information to be destroyed must be locked to prevent access to its contents.
- Digital Media (tape, CD/DVD, and flash drive): shredded.
- Hard drives: erased using a Department of Defense standard for data destruction or physically destroyed.
- Hardcopies (paper receipts, paper reports, and faxes): cross-cut shredded, incinerated, or pulped.
- Outsourced destruction of media must use a bonded Disposal Vendor and include logging/tracking when sent via secured courier or other delivery method.

IT Systems

<u>System Configuration</u>

All servers and network devices on USI networks, whether managed by employees or by third parties, must be built and deployed in accordance with this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the CIO.

- All systems are created via system intake process.
- All systems must be documented for initial build and subsequent updates and patches in the asset inventory tracking system.
- All systems commonly affected by viruses such as servers, workstations and laptops on USI networks, whether managed by employees or by third parties, must be configured with IT Security approved anti-virus software.
- All systems must have a defined backup plan.
- All systems must log access control events, the audit trail must be secured, and history retained.
- All system patches and updates must be reviewed for significance and appropriately applied, and vulnerabilities managed as defined in the Vulnerability Management section.
- All systems must adhere to firewall requirements as stated in the Firewall and Router Security Administration section.

<u>Firewall and Router Security Administration</u>

All server firewalls and all network firewalls and routers on USI networks, whether managed by employees or by third parties, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the CIO.

System Administrator Responsibilities

- Assuring changes to hardware, software, and security rules of firewalls and routers are included in IT Security Change Control
- Enabling appropriate logging on all security systems and performing active daily monitoring of the logs that report security events.
- Providing IT Security with read-only access to security event logs.
- Reporting network and server security incidents to IT Security immediately upon discovery.
- Ensuring that server firewalls and network firewalls and router configuration files are secured and synchronized properly.

Software Development

All development efforts of software designed to run on USI Enterprise Resource Planning (ERP) computing systems, whether managed by employees or by third parties, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the CIO.

ERP systems have a test/development environment, separate from the production environment, used to test all new software. If the test environment has connectivity with the production USI network, access controls must be in place to enforce the separation. If the test system uses data copied from production systems, then the same data and systems security enforced on the production system must be enforced on the test system.

Managed Detection and Response (MDR)

IT Security with support from the MDR provider and the Student Security Operations Center (SOC) is charged with protecting the University's electronic information assets, including performing ongoing, routine network security monitoring and using technologies to detect and/or prevent network intrusion.

IT Security may use the following monitoring technologies on the USI network:

- Intrusion Detection
- Intrusion Prevention
- Firewalls
- Network layer antivirus and anti-malware
- Network layer advanced threat protection
- URL / IP based reputation filtering
- Data Loss Prevention
- Netflow traffic monitoring.

Vulnerability Management

All servers and network devices on USI networks, whether managed by employees or by third parties, must be built and deployed in accordance with this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the CIO.

Critical servers and network devices are routinely scanned for known published vulnerabilities. Identified vulnerabilities are reviewed weekly for significance and are appropriately applied. Designated industry websites are reviewed weekly for security advisories.

Encryption

This policy documents encryption standards that must be used on all applicable mechanisms and systems on USI networks, whether managed by employees or by third parties.

Encryption is required for all laptops, and workstations that may be used to store or access critical and restricted information. Portable drives may only be used to store or access critical and restricted information if an approved encryption solution is available.

Critical and restricted information must be encrypted during transmission over networks in which it is easy and common for the data to be intercepted, modified or diverted (such as the Internet, wireless network, GSM, and GPRS). Some examples of strong encryption that is acceptable are:

- Transport Layer Security (TLS) v1.2 or higher
- Internet Protocol Security (IPSEC)
- SSH-2 or higher with a 2048 bit or larger key

The encryption technology used must only accept trusted keys and/or certificates, use secure configuration and not use insecure versions. The encryption strength must be strong and based on vendor recommendations or industry best practices. Any exceptions must be authorized by CIO/CISO.

Physical Security

This policy applies to the physical security of the university's information systems. Campus and Data Center Security controls include:

- Cameras or other logged access control mechanisms are used to monitor data center entry and exit points. The data collected is stored for at least 3 months unless otherwise restricted by law.
- Physical access to the data center is controlled with two-factor access.
- The data center is protected by fire suppression system, climate and moisture alert system, and UPS backup system.
- Data center visitor log is maintained.
- Campus network closets are key access controlled.
- Campus network jacks are controlled and not available for public access.
- Campus wireless network is logically separated from the main campus network and has independent security and access control.

Vendor Management

For all third parties with whom critical and restricted data is shared (e.g., back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), the following must be done:

- Maintain a list of all the third parties with whom critical or restricted data is shared.
- Written agreement that includes an acknowledgement by the third party of their responsibility for securing critical or restricted data. At a minimum these include:
    - Statement of data ownership
    - Statement of how and what format data is returned to the University
    - Statement of how vendor assesses its security
    - Statement of data destruction
    - Statement of location of data storage
- For agreements involving identity theft Red Flag covered accounts, include policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Email

Email should never be considered a secure technology and users are asked to exercise common sense when sending or receiving email from USI accounts. Additionally, the following applies to the proper use of the USI email system. Data classified as critical or restricted is never to be sent through the public Internet using unsecured end-user messaging technologies such as e-mail, instant messaging, or chat. Data classified as critical or restricted may only be transmitted via e-mail if secured by University approved encryption technology. Any exceptions must be authorized by CIO/CISO.

See Data Communication and Computer Use policy for additional email use details.

Network Access and Authentication

This policy applies to the network access and authentication of the university's information systems. Exemptions from this policy will be permitted only if approved in advance and in writing by the CIO.

User Access

Every user is provided a unique user account and must maintain a personal secret password. Multi factor authentication (MFA) is deployed for remote and web-based access to USI information systems and networks. Systems requiring the use of MFA include, but are not limited to, virtual private network (VPN), systems utilizing Single Sign-On (SSO), system administration tools, and privileged domain accounts. Employee user accounts are originated via Human Resources. Student user accounts are generated via the application process. Any user account requested outside this process requires CIO/CISO review and approval.

The use of non-authenticated (e.g. no password) user accounts is prohibited. User accounts not associated with a single identified user, such as a shared or group user account, are generally prohibited. Exceptions to user accounts associated with a single identified user must be evaluated, documented, and approved by CIO/CISO.

Each user's access privileges must be: authorized according to business needs, restricted to least privileges necessary to perform job responsibilities and assigned based on job classification and function. Departments requesting specific privileges complete an IT Resources request form. Requests for user account with system administration rights requires CIO/CISO review and approval.

Users accessing USI systems remotely: before establishing a connection the user must ensure the remote device is up-to-date on patches and is running a current anti-virus program. Once connected user must never copy or download data classified as Critical or Restricted to an unencrypted remote device.

Desktop Administrator Access

Under certain circumstances, Desktop Administrator Access may be issued to employees on either a temporary or ongoing basis to perform tasks within the scope of their employment. USI recognizes that issuing Desktop Administrator Access to computers introduces an increased risk to the security of its systems and data. Therefore, requests for ongoing Desktop Administrator Access must be accompanied by an approved authorization from the employee's department head or dean and the CIO.

The use of these rights and the level of access to the computer are to be in accordance with USI's Acceptable Use Policy. Desktop Administrator Access will only be granted on a very limited basis and only when absolutely necessary. Desktop Administrator Access will not be granted primarily for reasons of employee convenience.

Annual administrator access recertification process is coordinated by IT Security. A review of service accounts that are used as database application IDs must be included to verify that the service accounts can only be used by the applications and not by individual users or other processes.

Vendor and Guest Access

Vendor or Guest access is provided as needed to any person who demonstrates a reasonable business need to access the network. Guests and Vendors must agree to and sign the USI Acceptable Use Policy before access is granted. Vendor accounts used for remote maintenance must only be enabled during the time that access is needed and monitored while being used. Vendor and Guest accounts must be disabled at the end of the noted term. Extensions must be requested through CIO/CISO.

System Administrator Responsibilities

The System Administrator has the following responsibilities regarding user account and access management. Exemptions from this policy will be permitted only if approved in advance and in writing by the CIO.

- When someone leaves or transfers to a new role, access privileges for that role are removed from the user account. If requested, direct manager or Dean of Students access will be allowed for 30 days to both the network storage and email box of the user.

- When a password is established for a user, this password must be set to a unique value for each user and in compliance with the password rules and the user must be instructed on how to change the password.
- IT personnel with password change responsibilities must validate the identity of users before performing a password reset. The approved means for validating identity at USI is by doing it in person with a valid ID, or remote validation achieved by providing uniquely identifying pieces of information.
- Systems Administrators must use a secondary account with elevated privileges when performing any system administration function and are not permitted to use their regular user account. Secondary accounts must be disabled immediately when the user leaves or transfers to a new role.
- Ensure all systems and access to any databases containing critical or restricted data is authenticated (e.g., users, applications, administrators, etc.). Additional provisions are implemented for any end user workstation that has internet access such that direct access to restricted data is not permitted. User direct access or queries to databases must be restricted to user accounts on an as needed basis and requested via the IT Resources Request form.

Identity Theft Red Flags Program

The identity theft red flags program is designed to provide information to assist individuals in 1) detecting, preventing, and mitigating identity theft in connection with the opening of a "covered account" or any existing "covered account" or who believe that a security incident has occurred and 2) reporting a security incident. This program was developed pursuant to the Fair and Accurate Credit Transactions Act of 2003 and the Federal Trade Commission's Red Flags Rule, which require creditors to adopt policies and procedures to prevent identity theft.

Covered accounts maintained by the University of Southern Indiana include:

- Bursar/Student Accounts
- Stored Value/Eagle Access ID Cards
- Payroll Cards

Identification of Red Flags

Broad categories of "Red Flags" include the following:

- Alerts - alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies
- Suspicious Documents - such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied
- Suspicious Personal Identifying Information - such as discrepancies in address, Social Security Number, or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information
- Unusual Use or Suspicious Account Activity - such as material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges
- Notice from Others Indicating Possible Identify Theft - such as the institution receiving notice from a victim of identity theft, law enforcement, or another account holder reporting a fraudulent account was opened

Detection of Red Flags

Detection of Red Flags in connection with the opening of covered accounts as well as existing covered accounts can be made through such methods as:

- Obtaining and verifying identity
- Authenticating customers
- Monitoring transactions

An information security incident that results in unauthorized access to a customer's account record or a notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent USI or to a fraudulent web site may heighten the risk of identity theft and should be considered Red Flags.

Response to a Red Flag

Any suspected Red Flag detection needs to be reported to CIO/CISO for support in the Information Security Incident Response Process. Based on the type of red flag, the appropriate IT Security team member will work with the employee and Public Safety to determine the appropriate response.

Security Incident Reporting

Any employee who believes that a security incident has occurred must immediately report the suspicious activity to the IT Help Desk.

Service Providers

USI remains responsible for compliance with the Red Flag Rules even if it outsources operations to a third-party service provider. The written agreement with the third-party service provider shall require the third-party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities. Including notification to USI if a Red Flag is detected and the steps implemented to prevent or mitigate additional identify theft.

Training

All employees who process any information related to a covered account shall receive training on procedures as outlined in this document. Additionally, refresher training may be provided annually.

Red Flag Definitions

Covered Account - A consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition or fee installment payment plan.

Creditor - A person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit.

Identity Theft – A fraud committed or attempted using the identifying information of another person without authority.

Red Flag - A pattern, practice or specific activity that indicates the possible existence of identity theft.

Security Incident - A collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

Information Security Incident Response

A security incident may come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing restricted or critical data. The Information Security Incident Response Process (ISIRP) is a series of steps taken from the point of problem identification up to and including, final resolution and closure of a security incident. The process also contains information required to inform appropriate parties of the detection, problem status, and final resolution of the event. All employees have the responsibility to assist in the incident response process within their particular areas of responsibility. The scope of this policy covers all information assets owned or provided by the university, whether they reside on the network or elsewhere. The ISIRP communicates the flow of information and provides action guidelines for management, technical staff, employees, and students to follow regarding the notification and resolution of an IT security incident.

Examples of potential IT security incidents that an employee might recognize in their day-to-day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing logs, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Possible indicators include inaccurate information within databases, logs, files or paper records.
- Abnormal system behavior (possible indicators include unscheduled system reboot, unexpected messages, and abnormal errors in logs or on terminals).
- Security event notifications (e.g., file integrity alerts, intrusion detection alarms, and physical security alarms).

Roles and Responsibilities

Individual or Team	Role and Responsibilities
Employee	Aware of potential IT security incidents and report suspicious activity to the IT Help Desk
IT Help Desk	Receive initial report of a problem and gather relevant information
CIO or CISO	Single point of contact for status updates
IT Department	Analyze initial report and follow procedures to coordinate with CIO and IS, system administrator, or third party vendor to provide forensic support as needed and fix and restore service to normal
Security Team	Make leadership and management decisions or escalate to executive management regarding IT security incident and assist with determining appropriate course of action

Process Flow

#	Activity	Responsible Party	Within Timeframe
1	Help Desk or IT team member receives initial report	Employee, Student, Faculty, Help Desk, IT Department	N/A
2	IT help ticket created with details from initial report	IT Department	Initial Contact
3	Evaluate contents of initial report and determine additional IT resource needs	IT Department	Within 1 business hour of step 2
4	If IT review validates initial report as an IT security incident notify CIO and CISO. Add "ISIR:" to the help ticket and place it in IT Security queue	CIO, CISO, IT Department	Within 1 business hour of step 3
5	IT Security notifies the Security team and ensure IT team members are engaged	CIO, CISO, Security Team	Within 1 business hour of step 4
6	IT department and Security Team develop course of action	CIO, CISO, IT Department, Security Team, ISIR PR	Within 2 business days of step 4
7	IT Security produces Incident Report and conducts incident debrief	CISO	Within 2 business days of incident resolution

IT Security Incident Resolution- Analysis and Assessment (including but not limited to):

- Identify impacted hardware or network components
- Outline types of data impacted
- Consider any impacted trust relationship between the system servers, network components, subnet
- Identify impact to disabling compromised components
- Preserve the evidence
    - If the incident involves a compromised computer system, do not alter the state of the computer system.
    - Capture supporting logs (firewall, router, server, IDS)
- Classify IT security incident:
  The Security Team will assess the details provided and include the initial potential impact level.

Low - One instance of potentially unfriendly activity (e.g., port scan, corrected virus detection, unexpected performance peak, etc.).

Medium - One instance of a clear attempt to obtain unauthorized information or access (e.g., attempted download of secure password files, attempt to access restricted areas, single computer successful virus infection on a non-critical system, unauthorized vulnerability scan, etc.) or a second low attack.

High - Serious attempt or actual breach of IT security (e.g., multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, successful buffer/stack overflow, successful unauthorized access to sensitive or critical data or systems, stolen sensitive documents, etc.) or a second medium attack.

IT Security Incident Resolution- Decision, Action, Remediation (including but not limited to):

- Isolate attack (if intrusion is ongoing)
- Ensure the loss is contained
- Identify system vulnerabilities that allowed the intrusion
- Attempt to identify attacker
- Determine necessity of disabling the system or specific machine
- Determine restore and rebuild needs
- Determine impact to end user- the amount of time they will not have access to site, machine, or function
- Determine University impact
- Identify ISIR public relations contact (ISIR PR)
- Perform restores and/or rebuilds
- Update IT security incident classification:
  Incident classification escalation levels (including notification targets)

Impact	Description	Notification
High Impact	◦ Multiple systems are offline causing loss of business continuity ◦ Systems with data exposure ◦ Accounts compromised with access to critical data	◦ CIO/CISO ◦ Security Team ◦ DG ST ◦ Human Resource ◦ Insurance ◦ Legal ◦ Public Relations
Medium Impact	◦ One or more systems are under attack ◦ Unconfirmed data compromise ◦ Multiple accounts attempting compromise	◦ CIO/CISO ◦ Security Team
Low Impact	◦ Business email compromise ◦ Workstation malware compromise ◦ Lost or stolen device	◦ CIO/CISO

IT Security Incident Resolution- Corrective Action and Lessons Learned Review (including but not limited to):

- For each incident, Security Team will determine incident severity classification
- Implement identified corrective action items that assist with prevention of future recurrence
- Reflect on the incident. What are the lessons learned? How did the ISIRP perform? Was the policy adequate? What could be done differently? Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Contact List

Contact	Primary	Backup
Help Desk	812-465-1080	N/A
CIO	TBD	Stacy Draper 812-465-1063
CISO	Stacy Draper 812-465-1063	Lance Woods 812-461-5410
Security Team	TBD	Primary: Steve Bridges, Brad Will, Dave Alexander, and Lance Woods Contact Risk Management (Mark Logel) for Cyber Insurance support Secondary: Data Governance Strategic Team Members

ISIRP Training and Awareness

- Annually, in absence of actual ISIRP event, perform table-top exercise to facilitate education process and possible policy revision.
- Action items noted during actual ISIRP event or table-top exercise are reviewed and if needed incorporated into the policy
- Annually, IT Security performs legal requirements review and if needed incorporates into the policy
- Annually report ISIRP incidents to the Security Team

Revision History

Revision #	Description	Approval	Date
1.0	New policy	S. Draper- Author; IT Security Team and S. Bridges- Approved	7/31/17
1.1	Red Flags Addition	S. Draper- Author; IT Security Team and S. Bridges- Approved	6/15/18
1.2	MFA, MDR Addition and General Edits	S. Draper – Author IT Security Team and S. Bridges - Approved	1/14/22
1.3	CIO Resource Addition and General Edits	S. Draper – Author IT Security Team and S. Bridges - Approved	2/28/23
1.4	Enhanced ISIR and General Edits	S. Draper – Author IT Security Team and S. Bridges - Approved	6/20/24