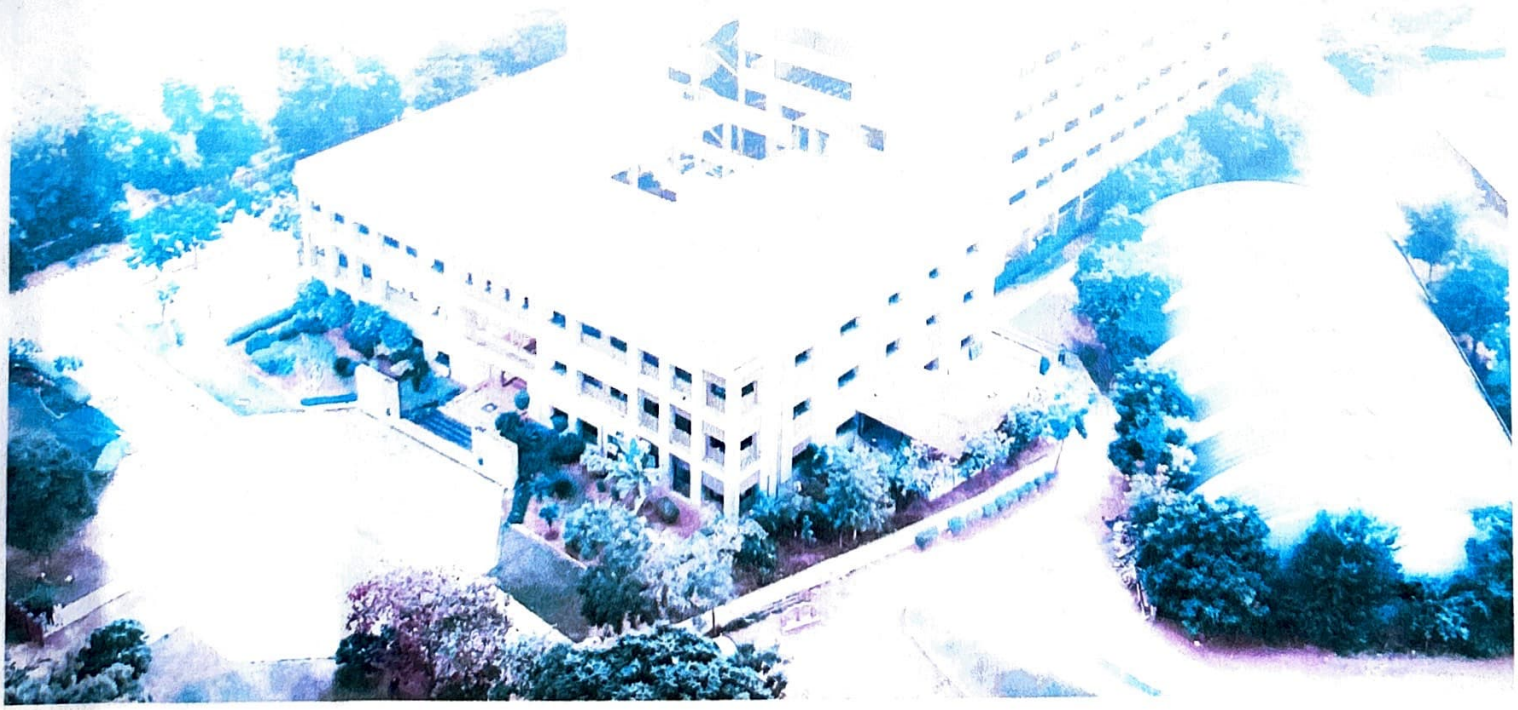
SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Swarrnim Startup & Innovation University

IT SOP



SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE.
INDIA'S FIRST UNIVERSITY FOR STARTUP

IT POLICY
2023-24

INDEX

11.	Policy Number: IT-16	Roles and Responsibilities for Information Security
12.	Policy Number: IT-17	Backup and Recovery Policy
13.	Policy Number: IT-18	Information Security Framework
14.	Policy Number: IT-19	Institutional Data Access Policy
15.	Policy Number: IT-20	The University of Iowa Airspace Policy
16.	Policy Number: IT-21	Computer Data and Media Disposal Policy
17.	Policy Number: IT-23	Computer Security Breach Notification Policy
18.	Policy Number: IT-24	Wireless Networking Policy
19.	Policy Number: IT-25	Network Address Allocation Policy for IPv4
20.	Policy Number: IT-26	Web Accessibility Policy
21.	IT - STANDARD 02	Enterprise Login ID Standard (SSIUID)
22.	IT - STANDARD 05	Computer Security Standard
23.	IT - STANDARD 22	University ID Number Standard

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-01
Scan-Pen-Test

Description:

Network scans of campus systems and devices are conducted for the purpose of general security and vulnerability assessment. The policy grants authorization to appropriate members of the Information Security and Policy Office and Health Care Information Systems' IT Security Office to coordinate and conduct Vulnerability Assessments and Penetration Testing against organizational assets.

Network Vulnerability Scanning and Penetration Testing:

Good security practices must be developed in conjunction with regular feedback on their effectiveness. One form of feedback can be produced using network-based security scanning tools. Regular scanning of devices attached to the network, to assess potential security vulnerabilities, is a best practice for managing a dynamic computing environment. For critical enterprise systems or those dealing with sensitive data, additional testing methods to look deeper for more security vulnerabilities may be a requirement for compliance with laws, regulations, and/or policies. One of these methods is Penetration Testing, which is targeted at systems by IT security experts, and is typically performed at the request of business owners.

Scope:

All devices attached to the University of Iowa's network are subject to security vulnerability scanning and/or penetration testing. In today's changing environment, vulnerable and/or unprotected systems can easily be overlooked. Systems that are not properly managed can become a potential threat to the operational integrity of our systems and networks. Vulnerability scanning can be proactive or reactive:

Proactive security scanning allows for a meaningful assessment of system security against known risks, provides a roadmap of effective countermeasures for improving security, and also provides a simple quantification of assets. Reactive security scanning allows for threat quantification and assessment, accelerated damage control, and an assessment of systems against reasonable control measures during the repair/rebuild process.

Any critical enterprise systems of the University are subject to periodic vulnerability assessments. Any system dealing with information governed by laws, regulations, and/or policies that require penetration testing are also covered. Other systems dealing with sensitive data may be submitted for penetration testing at the request of the business owner, or at the recommendation of the University Information Security and Policy Office.

Penetration testing is a separate and distinctly different set of testing activities. Its primary focus is the exploitation (not just observation or assessment) of security vulnerabilities and therefore may be disruptive of operations (some exploits may cause operating systems or applications to "crash"). Penetration testing is most beneficial when executed after an Assessment has been performed and the issues found by that Assessment have been remediated.

Policy Statement:

Multiple levels and types of network security scanning are utilized by the University of Iowa, and are managed as services offered by the Information Security and Policy Office:

1. Focused Scan-- Low-level scans for basic service-tracking purposes will be conducted on all networks in the University ssiu.ac.in domain. In addition, specialized scans to target specific problems posing a threat to the University's systems and networks or to correlate interrelated network-based vulnerabilities will be conducted on an ad-hoc basis. Focused scans are not typically advertised.
2. Recurring Group Scan – Groups of systems or departments identified as critical to the University, or that might subject the University to heightened risk will be subject to frequent, in-depth security scans. Any department can join the recurring group scan service upon request. Scan schedules are arranged with the system owner.
3. Ad Hoc Scan – Before a new system is put into service, it is recommended that a network security scan be conducted for the purposes of identifying potential vulnerabilities. Scans may be requested by system administrators at any time, as frequently as necessary to maintain confidence in the security protections being employed. Any system identified in conjunction with a security incident, as well as any system undergoing an audit may be subject to a network security scan.
4. Penetration Test - All penetration testing of University systems must be arranged by senior management/departmental business owner(s) and coordinated through the Information Security & Policy Office. Penetration testing is typically conducted over a period of several weeks, with regular feedback to the business owner(s) if issues are identified.

- Due to the more intrusive nature of a penetration test, and to better manage risks associated with such tests, a signed non-disclosure agreement and confidentiality agreement is required prior to commencing the penetration test. (see Related Policies, References and Attachments below for more details.)
- Penetration testing may be performed by any qualified service provider approved by the ISPO.

- High risk issues must be remediated in a timely manner, or units can work with the Information Security & Policy Office toward implementing compensating controls to reduce risks highlighted in the report(s).

Network scans will be conducted by *authorized scanning systems*: it security1.its.ssiu.ac.in, itsecurity2.its.ssiu.ac.in, itsecurityn.its.ssiu.ac.in in order to be easily recognizable as benign activity in system log files.

Related Policies, References and Attachments:

- This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
- They are incorporated into the University of Operations Manualreference, per the Policy on Acceptable Use of Information Technology Resources

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-02
Enterprise Active Directory

Description:

Authoritative directory source for other campus directories.This document sets forth the basic operational policies, guidelines and rules for the University of Iowa Enterprise Active Directory (AD) environment. The AD environment is integrated into the University's comprehensive network infrastructure, and includes Microsoft Domain Naming Service, as well as Active Directory Service. Information about people, applications, and computing resources is distributed throughout the University and Hospital information systems. Our campus and hospital networks have evolved from loose collections of connected devices to a complex, integrated system made up of interdependent resources. As a result, contemporary operating systems need to be able to manage the relationships between distributed network resources. Recognizing the importance of directory services to assist the campus IT community, ITS developed an Enterprise Directory Service, using LDAP standard access, integrated with authoritative sources and systems of information. This directory (currently Secure way from IBM, running on an AIX platform) was put into production in November 2000. It has requisite redundancy and security. It now becomes an authoritative source for other directories that may be necessary to enable specific vendor strategies or applications. One such directory, Active Directory, an integral part of Microsoft's newest operating system Windows 2000, is required to derive full benefit from Microsoft products. A collaborative process of designing AD architecture, policy and management of domains at an enterprise or campus-wide level has been developed for the implementation of Active Directory for both the hospital and the campus. The technical basis of this design is the result of an inter-collegiate project (facilitated by Microsoft Consulting Services and led by ITS).

Scope:

This policy apples to all campus IT provider that utilize Windows devices connected to the campus network. It is the collaborative consensus of policy and practice for the design, implementation and management of shared services. The technical manifestation of the architecture is the single forest, which contains all the domains on the campus. No other forests will be recognized by the campus network, unless approved under this policy. Compliance with these guidelines is essential to the coordinated operation and expansion of services for the

Swarrnim Startup & Innovation University ★ Gandhinagar

benefit of the full campus and hospital community of users. Changes to the policy and practices can be made as situations warrant, through the oversight committee defined below.

Policy Statement:

I. Governance - The creation, oversight and daily operation of this policy is vested in the following groups, in concert with existing IT providers.

Enterprise IT Committee

The primary advisory structure for the operation of enterprise wide projects and shared services is the Enterprise IT Committee (EITC). The EITC is responsible for oversight of the campus Active Directory forest. In addition to policy, Active Directory version upgrades and feature sets will be deployed at the direction of the EITC.

Active Directory Enterprise Administrators:

The primary administrator group at the enterprise operational level is the Active Directory Enterprise Administrators (ADEA or Enterprise Administrators) group. The initial membership of this group is included in the attachments. The primary orientation of the Enterprise Administrators is to the operation and maintenance of the University of Iowa Active Directory forest, only. The group is a small, trusted set of individuals that work closely as a team to provide reliable, 24 x 7 operation of the UI forest and support for AD domains, as required to preserve the health of the forest. Due to the University-wide responsibilities of this group, the employing unit for each ADEA member must concur and support these global responsibilities. This means that sufficient time for forest administration, continuing professional education, and status reporting must be made the highest daily priority for each member. It is possible that this could be a full time commitment of the individual, depending on operational demands.

Enterprise Administration Responsibilities

- Active Directory Enterprise Administrators have full access to the root of the University of Iowa Active Directory forest. They are responsible for the daily operation of the AD forest.
- Enterprise Administrators are also responsible for the DNS services running on the forest root domain controllers. It is expected that any changes will be planned and executed in collaboration with ITS Telecommunication and Networking Services (TNS) staff, as required.
- Because of the nature of access and institutional responsibilities, members of the Enterprise Administrators group serve at the discretion of the EITC. New members will be considered

Swarrnim Startup & Innovation University Gandhinagar

through the nomination of trusted administrators. A nomination of a new administrator must be unanimous among the existing enterprise administrators.

- Three to five individuals may be assigned to the ADEA, with a six-month probationary period. Enterprise Administrators are expected to work as a team and serve as mentors to other campus AD domain and OU administrators.
- Representative responsibilities of the ADEA are documented in the "Active Directory Enterprise Administrator Handbook".
- The ADEA will regularly report to the EITC about its activities and health of the forest. Detailed problem and change logs will be an essential part of such reporting.

Domain Administration Guidelines

- Domain Administrators have full responsibility and administrative control of a specific Active Directory domain within the University of Iowa forest. Each domain must have at least two experienced full-time information technology professionals identified to be the domain administrators.
- Domain Administrators must be good Active Directory citizens. Domain Administrators are responsible for supporting the operation of the campus forest by maintaining the good health of their domain. Domain Administrators must respond to ADEA requests to correct any problems that impact the forest.
- DNS for each Active Directory domain will be the responsibility of the respective domain administrators, again in collaboration with ADEA and TNS, as required.
- Domain Administrator assignments are made by the IT manager/director for the college or administrative unit, subject to the issues covered by this policy.

Enterprise Exchange Administrators

The Enterprise Exchange Administrator Group (EEA) is responsible for enterprise-level Exchange related activities. Active Directory does not allow the ADEA to delegate all of the necessary rights to the local Exchange administrators. These Exchange support activities are performed by the EEA.

II. Single University Active Directory Forest

The Active Directory forest is the top-level logical entity in Windows. Within the forest is a collection of domains that share a common infrastructure. The University has selected a single forest model because it presents the best opportunity to provide a consistent interface to the end-user from anywhere on the network. One of the characteristics of a single forest is the sharing of information between Exchange calendars. This model requires considerable agreement on policy and operational processes to be successful.

The operation and nature of the forest relationships is not directly tied to political, organizational or economic structures. The goal of the forest is that interoperability by all relevant individuals and systems is enhanced by their membership. It certainly includes faculty, staff and students, and may include patients, distance education students, alumni, and others as appropriate. To that end, inclusive approaches will be established to promote participation in the UI AD Forest. Likewise, attempts to establish alternative forest structures will not be supported.

Organizational Units in a Domain

It is our goal to minimize the number of domains for a variety of technical, reliability and economic reasons. There will be many instances in which a new organizational unit (OU), with delegated authorities will be fully sufficient, instead of a new domain. Any campus unit wishing to establish a new organizational unit within an existing domain may do so by contacting an administrator of an existing domain or ADEA member.

Domain Creation Guidelines

The simplest structure is the strongest. The most robust, supportable forest infrastructure is the one that minimizes the number of individual domains. However, there are technical and political reasons that can only be met by the establishment of multiple domains within the single forest.

The process for determining whether a new domain is appropriate for a college or organizational unit wishing to join the forest is based on factors such as:
Ability of requestor to substantially leverage Microsoft W2K/NT resources.

- Availability of qualified IT staff, trusted by peers outside the unit.
- Availability of adequate hardware dedicated to support of the domain.
- Commitment to the operational processes of the forest, including an emergency reporting and response staffing structure.
- Specific functionality requirements that cannot be met by an Organizational Unit (OU)

Meeting the minimum requirements for domain admission does not automatically guarantee that an organization will be allowed to establish a separate domain in the Active Directory. The

Swarrnim Startup & Innovation University Gandhinagar

ADEA will balance the wishes of the requestor with the health of the enterprise forest. Assistance will be provided by the Enterprise Administrators to help install and configure all new domains, so that they integrate properly with the existing environment.

Active Directory Domain Name Service (DNS)

The primary purpose in defining DNS responsibilities is to deploy the most robust and feature-rich environment possible, without reducing the reliability and effectiveness of the existing campusnetwork.

TNS provides the campus DNS oversight and management. Primary DNS for the forest root domain will be implemented and managed by the Enterprise Administrators. DNS authority for the forest root domain is delegated by TNS from the BIND servers hosting the primary SSIU.AC.IN domain DNS services. The forest DNS is hosted on Windows domain controllers in the Active Directory forest root. TNS, in collaboration with the Enterprise Administrators, will determine DNS updates required to support decisions to add domains to the forest. Actual changes to DNS on the forest root domain controllers will be made by an AD Enterprise Administrator in collaboration with TNS. DNS administration for each Active Directory domain (other than the root domain) will be the responsibility of the respective Domain Administrator, again in collaboration with both ADEA and TNS, as required.

Schema Change Management :

Because the schema of the AD is a shared resource, with mission-critical dependencies built into its structure, all changes will be submitted to a rigorous Schema Change Management process. While this may require negotiation of desired attributes with other users, it is essential to sustain the reliability of the directory. Required characteristics of this process: Identifying needed changes, documenting the need for changes, testing schema changes, documenting test results, and presentation of results, before implementation.

Request for schema changes are submitted to the ADEA. After evaluation and assessment by the ADEA, a recommendation for implementation timing, the precise specification of the change, and an assessment of impact on all AD users will be made to the EITC. EITC approval is required before any changes are implemented. Testing of the change is required, but may occur before or after the ADEA recommendation.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.

They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information...)

- Enterprise Password Policy
- Enterprise Login ID Standard
- Active Directory Enterprise Administrator Committee

Policy Number: IT-05
Enterprise Password

Description:

A password is a sequence of characters required for access to a computer system or service.

A passphrase is a long password, typically constructed from a sequence of words – a song, poem or phrase, employing the use of characters, spaces and symbols.
Many computer systems and applications at the University of Iowa use a login ID and password (or passphrase) as the method of authenticating users. As the university moves toward a single-sign-on environment, where entry of a single login ID and password authenticates you to multiple systems, a robust passphrase provides a major defense against unauthorized use of our systems. The object when creating a password is to make it as difficult as possible for others to make an educated guess or to programmatically "crack" what you've chosen. An effective method of accomplishing this is by using a "passphrase" form of password. For example, using several words together, or the first letter of several words from a memorable sentence, event, quote, or song lyric, combined with the other minimum password standard rules, as defined in this policy, can create a strong and sufficiently long passphrase that is easily remembered. You can protect your own files and University resources by choosing a good passphrase, changing it regularly, and never sharing it with others.

Policy Statement:

This policy applies to all information technology systems and processes at The University of Iowa that create, modify, or use information that is private/confidential or of significant institutional value. All such systems will adhere to the minimum acceptable standards, as described below.
System administrators may choose to implement these standards with a combination of technological controls and local practice. Policies and/or standards adopted by a college or administrative unit must be consistent in principle with this University policy, but may provide additional detail, guidelines or restrictions.

Part 1: Minimum Password/Passphrase Standards (for all University accounts):

1. A unique user identifier and password is issued for each user of the system. The University SSIUID (HealthcareID for clinical applications) should be used when possible.
2. User-initiated password changes must be supported.
3. Sharing of your individual account ("SSIUID","HealthcareID") is prohibited. Passwords must be changed if they have been used, obtained, or suspected to be obtained, by anyone other than the account owner.
4. Passwords must be changed at least once annually (every 365 days).
5. Passwords must be stored in a hashed/encrypted format, and will be transmitted over open networks in an encrypted format.
6. Passwords must pass all of the following composition rules:
    1. A combination of alphabetic, numeric and special characters that does not match previous passwords, and
    2. A minimum of 9 characters, but recommend 15 or more characters passphrase, and
    3. At least one limiting characteristic is used (for example, no character string matches from previous passwords; no consecutive, repeated, or serial characters (e.g., aaaa1111, abcd1234); or no single dictionary words)
    4.

Part 2: Additional Password/Passphrase Requirements:

1. Elevated Privilege System Accounts.

Elevated privilege system accounts are those accounts that have the rights required to maintain a system or application – such as operating system, application, or database administrator accounts, or to operate a scientific instrument. Administrators should not use their SSIUID account as an elevated privilege system account. Each systems administrator should be assigned their own elevated privilege system account that is not shared, and is used only when the elevated privileges are required. Where possible these accounts should use a managed authentication service such as Active Directory, LDAP or RADIUS. When elevated privilege system accounts are accessed remotely, it is recommended that they are used as part of a multi-factor authentication service.

Elevated privilege system account passwords/passphrases will:

1. comply with the minimum password standards

Swarrnim Startup & Innovation University Gandhinagar

2. be changed at least semi-annually every 180 days)
3. be at least 15 characters in length when possible

2. SSIUIDs with Elevated Privileges.

The special password requirements above may also apply to SSIUID accounts that have been assigned a role with elevated privileges. For example this includes an account that has the authority to change other user passwords, or an account that has the authority to assign other users to elevated privilege roles.

3. SSIUIDs with Access to Sensitive Institutional Data.

Some SSIUID accounts are used to access sensitive institutional data – such as personally identifiable health information, or human subjects research data that identifies individuals. The Business Owner(s) of such institutional data may require these SSIUIDs to have passwords which meet the elevated privilege password requirements.

4. Local workstation administrator accounts.

The special requirements above also apply to local system administrator accounts where the password is stored on the workstation and account authentication does not rely on a central authentication service. Local administrator passwords should be unique per computer for computers covered by this policy. The local administrator account and password should only be used for system administration purposes.

5. Service accounts.

These are accounts where the password is managed within a work group, and include device passwords. Service accounts are subject to the elevated privilege account password complexity requirements but are exempt from the change requirement. These accounts should be reviewed annually to ensure that they are still required for proper operation. All service account passwords must be changed when a work group member who could have known the service account password leaves the work group.

Part 3: Other Requirements:

1. Assisted Password Resets: User account passwords will not be reset if the password administrator cannot identify the user requesting the password change/reset with one of the following:

A secret key or satisfactory answers about personal information held in central database records,
A supervisor or technology support person's personal vouch/identification,
A photo ID or human factor such as a biometric scan, or
Satisfactory challenge-responses in a self-service application

2. Policy Exception Process: University applications or services with an implementation that

2. be changed at least semi-annually every 180 days)
3. be at least 15 characters in length when possible

2. SSIUIDs with Elevated Privileges.

The special password requirements above may also apply to SSIUID accounts that have been assigned a role with elevated privileges. For example this includes an account that has the authority to change other user passwords, or an account that has the authority to assign other users to elevated privilege roles.

3. SSIUIDs with Access to Sensitive Institutional Data.

Some SSIUID accounts are used to access sensitive institutional data – such as personally identifiable health information, or human subjects research data that identifies individuals. The Business Owner(s) of such institutional data may require these SSIUIDs to have passwords which meet the elevated privilege password requirements.

4. Local workstation administrator accounts.

The special requirements above also apply to local system administrator accounts where the password is stored on the workstation and account authentication does not rely on a central authentication service. Local administrator passwords should be unique per computer for computers covered by this policy. The local administrator account and password should only be used for system administration purposes.

5. Service accounts.

These are accounts where the password is managed within a work group, and include device passwords. Service accounts are subject to the elevated privilege account password complexity requirements but are exempt from the change requirement. These accounts should be reviewed annually to ensure that they are still required for proper operation. All service account passwords must be changed when a work group member who could have known the service account password leaves the work group.

Part 3: Other Requirements:

1. Assisted Password Resets: User account passwords will not be reset if the password administrator cannot identify the user requesting the password change/reset with one of the following:

A secret key or satisfactory answers about personal information held in central database records,
A supervisor or technology support person's personal vouch/identification,
A photo ID or human factor such as a biometric scan, or
Satisfactory challenge-responses in a self-service application

2. Policy Exception Process: University applications or services with an implementation that

Swarrnim Startup & Innovation University ★ Gandhinagar

does not meet the minimum standards must be granted a policy exception. The approval process for exceptions requires the system owner to share a technical description and statement of justification for the exception. This information, and if necessary a security review, are subsequently analyzed and approved as appropriate by the University IT Security Officer. E-mail: it-security@ssiu.ac.in for more information.

3. Enforcement: All computer systems and processes subject to this policy are encouraged to incorporate a managed University authentication service for automated account and password management, or they must implement the password standards locally. Systems and processes that do not comply with this policy, and have not been granted an exception, will be subject to loss of access to the University campus network.

Related Policies, References and Attachments:

Enterprise Login ID Standard
Enterprise Authentication Policy
Network Citizenship Policy
Institutional Data Policy
Creating a Good Passphrase (http://its.ssiu.ac.in/support/article/2549)

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.

They are incorporated into the University of Iowa Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

Swarrnim Startup & Innovation University Gandhinagar

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-06
IT Security Incident Escalation

Brief description:

Provides guidance in determining the proper response to a misuse of or attack on IT resources from within or outside the University.

Introduction:

This policy provides guidance in determining the proper response to a misuse of IT resources from within or outside the University. It documents where to report problems and when to involve University administration, judicial representatives, and legal representatives. It also documents the individuals designated for these responsibilities, and procedural details, which depend on the severity and source of the attack.

Scope:

Attacks on University IT resources are serious infractions of the Acceptable Use of Information Technology Resources policy, and misuse or vandalism of University resources. We must pay particular attention to the education of our community with regard to proper behavior in these matters. Serious attacks on University resources will not be tolerated, and this policy provides a method for pursuing the resolution and follow-up for incidents.

Policy Statement:

The entity responsible for support of the system or network that has been compromised or is under attack is in all cases expected to:

1. Report the incident to the Chief Information Security Officer (see Attachment 2)

Swarrnim Startup & Innovation University Gandhinagar

2. Take action at the direction of the Chief Information Security Officer to contain the problem, and block or prevent escalation of the attack, if possible
3. Remediate changes, and repair the resulting damage
4. Restore service to its former level, if possible
5. Preserve evidence, as directed by the Chief Information Security Officer, where its deemed appropriate

Incident Scenarios Summary:

	Short Term Duration /Minor Damage	**Long Term Duration /Major Damage**
Source Originates Inside University of Iowa	Report to Information Security & Policy Office Assist in investigation as necessary Remediate or repair breach (close) Report to judicial representative for sanctions	Report to Information Security & Policy Office Preserve evidence Stop/Repair breach (close) Notify service provider(s) Report to CIO Report to judicial representative and/or General Counsel and/or Public Safety for follow-up
Source Originates Outside University of Iowa	Report to Information Security & Policy Office Repair breach (close) Send notice/complaint to service provider(s) if possible	Report to Information Security & Policy Office Preserve evidence Notify service provider(s) Pinpoint source if possible Stop/Repair breach (close) Report to CIO Report to General Counsel and/or Public Safety for follow-up

Related Policies, References and Attachments:___

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in/) by reference, per the Policy on Acceptable Use of Information Technology Resources.

Acceptable Use of Information Technology Resources Policy

https://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources
Computer Security Breach Notification Policy
https://itsecurity.ssiu.ac.in/computer-security-breach-notification-policy
Procedures for handling a computer system compromise incident
https://itsecurity.ssiu.ac.in/handling-it-system-compromise

IT Security Resources
https://itsecurity.ssiu.ac.in/resources
IT Security Resources

Attachment 1 - DETAILED RESPONSES:
Short Term Attack and/or with Minor Damage

- Attacks that are judged to be minor in scope or short term in duration, and originate inside the University, will be validated and if confirmed, reported to the appropriate judicial representative after one warning from the Chief Information Security Officer. The warning to the source explains that they are in violation of the University's Acceptable Use of Information Technology Resources Policy, and are being given one chance to modify their behavior. If the initial attack is relatively more serious, yet still "minor", the warning is to be waived and a report made to the appropriate judicial representative. This is a judgment call to be made by the Chief Information Security Officer.
- A judicial report will result in a permanent record of the attack, and a sanction(s) commensurate to the seriousness of the attack. The intent is to provide an opportunity for members of our community to learn that we take these matters seriously and will

not overlook inappropriate and potentially damaging behavior. Repeated attacks will result in escalation to policy regarding incidents having long term and/or major damage.

- Attacks which originate outside the University will be reported to the appropriate service provider by the Chief Information Security Officer if of sufficient seriousness to warrant action on their part. The service provider will be given detail regarding the attack in order that the attacker may be dealt with according to the service provider's terms of use. It is not economically feasible for the University to pursue additional action against attackers (or their service provider) for minor problems.
- When the source of a minor attack cannot be determined, because of a lack of evidence or because of faulty evidence, then it is in the best interest of the University to close the issue. (Evidence may be in the form of system recording (log) facilities, monitors, cache files, program dumps, network traces, disk storage media, etc.)

Long Term Attack and/or with Major Damage:

- In consultation with the Chief Information Security Officer, once the entity responsible for the system or network determines that an attack is of "major" consequence or damage, or the attack continues for a long duration (on-going or greater than one day), operational steps must be taken to preserve evidence. Major damage might be a loss (or corruption) of institutional data, an extended outage of a critical service or application, or other high-impact/high-cost damage.
- An on-going attack originating inside the University will be reported to appropriate campus service providers as soon as it is detected. If needed, that group will perform tracing through network analysis to pinpoint the source of the attack. Alternatively, if the attack is detected through networking analysis, it will be reported to the Chief Information Security Officer and the entity responsible for the system as soon as possible after its detection.
- If the source of the attack was outside of the University, ITS service providers will perform tracing through network analysis with the cooperation of the University's Internet Service Providers, and/or other external service providers. When external service providers are involved, an appropriately high problem severity level and rapid escalation procedures will be observed in order to trace the attack source and reach a resolution quickly.
- The Chief Information Security Officer will inform the University Chief Information Officer (CIO) of the attack in a timely manner. The appropriate judicial representative(s) will also be informed, based on the source of an attack that originates inside the University.

- University legal representatives, in consultation with the CIO, will make a judgment regarding the seriousness of the attack and the appropriate legal action. In all cases, the University will analyze the impact and pursue punishment for the attacker if the source can be pinpointed with sufficient evidence to prove wrongdoing and there is justifiable cost to recover.
- In the unlikely event that a long term event, attack or a major or critical system attack goes undetected, evidence is lost, and the attack cannot be traced to a source, then there is little to be done with the exception of recovery or repair of the damage and restoration of service. Serious attacks of this type will be reported as such to management for review.

Policy Number: IT-07
Residence Halls Network Acceptable Use (ResNet)

Description:

Rights and responsibilities of students using the Residence Halls Network.
As a student in the Residence Hall Network (ResNet), you will be connected to the campus network and the global Internet. This connection is a privilege, not a right. The University expects ethical and responsible behavior in the use of this network. That is, you are expected to be a good Internet citizen. Don't participate in any illegal or inappropriate activity or anything that will negatively impact the other users of the network.

Policy Statement:

Your use of all campus information technology resources, including this network, is subject to The University of Iowa Policy on Acceptable Use of Information Technology Resources, as well as to all other applicable University policies and state and federal laws. In addition, the following standards are in effect. This list is meant to be illustrative, not exhaustive.

1. Student is responsible for all activity originating from this connection. Student must take reasonable precautions to prevent unauthorized use by others of this connection, and his/her accounts, programs, or data.
2. Students should not engage in activities that consume excessive amounts of network bandwidth.
3. Student must not modify or extend Residence Hall network services and wiring. This applies to all network wiring, hardware, and in-room jacks. The only device you can

connect is a personal computer. You may not connect servers of any type, hubs, or network printers.

4. Residence Hall connections are provided for individual use only. Student may not create accounts on his/her computing system that provide campus network access for anyone else.
5. Residence Hall connections are for University-related activities only. Student may not conduct a commercial business via the Residence Hall connection.
6. Student may not run sniffers or any other software or hardware designed to intercept packets or to disrupt the security or operation of the campus network.
7. Student may not participate in illegal activities such as software piracy -- either the distribution of copyrighted software or illegal attainment of software or other copyrighted materials -- from the Residence Hall connection.
8. Student may not host chat lines from a computer connected to this network.

Enforcement:

At its discretion, the University may use its capability to examine network resources for violations of this policy. Sanctions for violation of this policy may result in disconnection from the campus network, other disciplinary action, or referral to external authorities.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)
1.Policies Affecting Students, Division of Student Services (https://dos.ssiu.ac.in/policies/)

Swarrnim Startup & Innovation University Gandhinagar

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

POLICY NUMBER: IT-08
DOMAIN-NAME-POLICY

Description:

Any computer or device physically connected to or accessing the University telecommunications network must be secured using baseline security standards to minimize disruptions to the operation of the network.

BRIEF DESCRIPTION: Any computer or device physically connected to or accessing the University telecommunications network must be secured using baseline security standards to minimize disruptions to the operation of the network.

Introduction:

The University of Iowa relies heavily on computers to meet its operational, financial, and information requirements. Network connectivity provides important functionality for these computing uses. In order to protect that functionality, it's important that persons owning, or overseeing the use of, devices connecting to the network assume responsibility for securing these devices to ensure that they don't disrupt the operation of the campus network.

Scope:

This policy governs all devices (e.g., server, desktop, laptop, handheld) that are connected to the campus network. Systems that are not properly administered can become a threat to the operation of the network. The responsibility for the security and integrity of the devices connected to the campus network initially rests with the person who connects the device to the network. Thereafter, the primary user of a computer shares responsibility with whoever provides IT support for that computer, followed by the department housed in the physical space the computer occupies. Technical staff who manage multi-user shared resources will have primary responsibility for them, followed by the department housed in the physical space the computers occupy. Faculty, staff, students, and other individuals (i.e., contractors, vendors, trainers, visitors) who have devices connected to the network, even if the devices are not owned by the University, as well as persons who have authorized the purchase of vendor operated and administered systems, are included as "system administrators" for the purpose of this policy.

Policy Statement:

The network citizenship policy is intended to protect the integrity of the campus network and to mitigate the risk and losses associated with threats to the campus network and networked resources. System administrators and users must

1. Follow University of Iowa Baseline Security Standards for securing network attached devices in order to ensure that key security vulnerabilities are addressed. Key vulnerabilities will change over time as new threats and risks emerge. Security standards will evolve in the same manner. See Appendix A for current Baseline Security Standards.
2. Cooperate with the University of Iowa Information Technology Security Office (it-security@ssiu.ac.in or 319-335-6332) to resolve security problems identified with any systems you are responsible for.
3. Submit network connected devices to vulnerability scans, and resolve high risk issues identified by the scans.
4. Immediately report compromises and other security incidents to the Information Technology Security Office (web resources at http://itsecurity.ssiu.ac.in/report-security-incident or call 319-335-6332) or report it to your local IT support staff.
5. Comply with the individual responsibilities stated in Section IV of the University's Acceptable Use Policy for Information Technology Resources.

Enforcement:

Systems posing an immediate threat to the campus network will be removed from the network to isolate the intrusion or problem and minimize risk to other systems, until the system is repaired and the threat is removed, as determined by the Information Technology Security Office. Systems involved in security incidents which do not have Baseline Security Standards implemented will remain off the campus network until the system administrator brings the system into compliance. Departmental Network and Security Contacts have the authority to remove devices from the network in their area of responsibility, and will be notified when systems in their department are removed from the network by central security or networking staff.

Systems that are involved in multiple incidents may be disconnected from the campus network for longer periods of time as required. System administrators will be required to show that they understand best practices and know how to implement them through an audit review or other assessment of their devices, before they will be allowed to reconnect them to the campus network. If a system administrator lacks the knowledge or training needed to comply with this

Swarrnim Startup & Innovation University Gandhinagar

policy, the Information Technology Security Officer will work with the department to help plan an appropriate training program for the system administrator.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contains acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.

They are incorporated into the University of Iowa Operations Manual (http://opsmanual.ssiu.ac.in/) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources).

Computer Vulnerability Scanning Policy
Information Security Framework Policy
Enterprise Password Policy
Security Best Practices Documentation

Appendix A: Baseline Security Standards

1. UPDATES: Keep all software (operating systems and applications) up to date to the extent possible (i.e., within compatibility and certification constraints). Configure devices to install security updates automatically, or perform the operation manually on a frequent, regular basis. Only use operating systems and applications that are actively supported. Software that isn't supported or that doesn't have recent security updates should not be directly connected to the campus network.

2.ANTI-VIRUS: Install anti-virus software on all eligible devices, using UI site-licensed software where possible, and make certain the virus detection signatures are updated on a daily basis. Configure the software to scan all incoming files.

3. ADMINISTRATOR PASSWORDS: Configure accounts with high-level system access (e.g., administrator or root) to have strong passwords that are changed often, consistent with the Enterprise Password Policy.

4. SUPPORT: Know who provides technical support for the computers you use. Department IT support staff, central (ITS) help desk, or other (contracted) support names, phone numbers, and/or email addresses should be known and available at all times. Register all systems that store Level III sensitive data with the Security Office.

5. BEST PRACTICES: Review and implement security best practices appropriate for the device in question. A collection of resources and documentation for best practices is available at the IT Security website.

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-09
Mass E-mail Mailings

Description:

Provide guidance and procedures for the use of large-volume electronic mailings to the campus community.

Electronic mail (e-mail) is an important resource for academic, research, and administrative communications. A targeted mass e-mailing is one method for delivery of information, though it may not always be the best choice (see "Mass E-Mail Support Center" below). Benefits of Mass E-Mail include speed of delivery, a facility for selection of "targeted" recipients, and the potential for enterprise-wide cost savings.

Policy:

The purpose of this policy is to provide guidance and procedures for the use of large-volume e-e-mail messages to the campus community. A "mass e-mail" is any single or group of identical mailings that goes to more than 1000 individuals, other than via self-subscribed mailing lists. Nothing in this policy is intended to interfere with faculty or collegiate communication with students.

Under Iowa law, the e-mail addresses of public employees are public records. Release of student e-mail addresses are governed by the federal Family Educational Rights and Privacy Act (FERPA). The University complies with Iowa and federal law in fulfilling requests for e-mail addresses, including the charge it imposes for the costs incurred in providing the information. Although individuals and/or organizations outside of the University may legally obtain University email addresses, our e-mail system is not intended for mass delivery of non-university related messages. The University uses services and techniques to protect against malicious e-mail, unsolicited ("spam") advertising, and targeted "phishing" scams. We reserve the right to take appropriate action to protect our systems and community members, including but not limited to blocking the delivery of e-mail and the sources that violate this policy.

All targeted mass e-mailings must be approved and processed using the guidelines described in this policy. Individual administrative areas may in addition, apply more restrictive rules on the frequency, acceptable purposes, approval procedures, and recipients of any campus communication.

Any faculty, staff or student who initiates a mass e-mail is accountable under both this po

and the policy on Acceptable Use of Information Technology Resources, specifically section 19.4.a Use Resources Appropriately.

Required Content for Mass E-mail Messages

1. All University of Iowa mass e-mail messages must include a University individual or group e-mail address to which a reply can be easily generated.
2. One of the approved category codes will appear on the subject line, which may be used by campus recipients to organize or filter their e-mail messages.
3. A notice that the message has been approved under the University's Mass E-mail Policy, with a reference to the "Mass E-Mail Support Center" that provides instructions for adjusting personal mail filters based on the category codes described above.

Targeted Mass Electronic Mailings:

Targeted group e-mail lets University of Iowa persons and organizations send a single approved message to a specific group of people, such as faculty, staff, or students, who can be identified based on characteristics in the enterprise directory or other institutional database.

1. The President of the University and members of the Vice Presidents Group may send mass e-mails to faculty, staff and/or students at their discretion, although notification of the appropriate Vice President and that Vice President's designee is recommended as a courtesy.
2. Leaders of the Faculty Senate, the Staff Council, and the Student Government may send mass e-mails to their particular constituent group at their discretion. They must obtain permission from the appropriate Vice President to send mass e-mails to other audiences.
3. Faculty and staff may request this service, with the approval first of their organizational leadership (e.g., Dean or Unit Director), and then the Provost or Senior Vice President and Treasurer, as appropriate.
4. Recognized student organizations may request this service with the approval of the Vice President for Student Life.
5. Faculty and staff organizations may request this service with the approval of the Vice President of the departmental sponsor.
6. Academic information may be e-mailed to groups of students (2000 or less) with the approval of the Registrar.
7. Time-critical messages may bypass some steps in this process provided permission has been granted by the President or appropriate Vice President.
8. Service messages that are directed to the customers of that service are exempt from this policy. These messages are sent at the discretion of the service owner.

9. The UI Institutional Review Boards have authority to authorize targeted e-mail for the purpose of recruiting subject participants for research studies, in place of the other authorizing officials.

Enforcement:

Failure of University faculty, staff or students to follow this policy and associated procedures may result in interruption of mail messages, loss of mailing privileges, and/or fees assessed for the cost of correcting any problems.

Faculty, staff and students are to use the Mass E-Mail Service rather than requesting data files of e-mail addresses, or sending mass e-mails themselves using the University directory. E-Mail addresses may not be sold, copied, distributed, or used for other than their intended purpose. Failure to protect this information is covered by the "Acceptable Use of Information Technology Resources" policy, including the sanctions defined therein.

Mail Originating Outside the University:

To protect the integrity of the University's e-mail infrastructure, anti-spam and anti-malware protection is used to delete, reject, clean, and/or quarantine messages that are determined to have high probability of causing a negative result to the service or persons using it. All e-mail messages delivered to the University are subject to these protections. The University e-mail system is not intended to be used for mass e-mail messages to community members for purposes that do not apply to our academic, administrative, or research missions.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.

They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

1. Mass E-Mail Support Center (http://its.ssiu.ac.in/support/article/3804)

Mass E-mail Request Form (http://apps.its.ssiu.ac.in/massmail2/beans/public.action)

Appendix A: Procedures:

Mail Sender	1. Read and understand the requirements and process of this policy

2. Develop the content of the message.
3. Develop a desired audience description and estimated size. Use the guidelines to determine if e-mail is the best choice for sending your message.
4. Submit the electronic message to ITS Mass Mail Service a minimum of seven days before the mailing date. (Note: For complex population requests, please allow for additional preparation and processing time, up to two weeks.)
5. Submit an "Approval Form for Mass E-Mail Request" to the departmental director, and Provost or V.P. responsible for the individual or group originating the message.
6. Obtain the approval of one or more of the following based on the intended audience and type of message:

- **Vice President for Student Life**
- All mass mailings to students
- Mailings to selected students about activities or student organizations
-

Associate Provost for Undergraduate Education and/or Associate Provost for Graduate Education

Mailings to selected students about academic matters, financial aid matters, or university admission

Executive Vice President and Provost

Mailings to faculty

Senior Vice President and University Treasurer

Mailings to staff, affiliates, and retiree

Institutional Review Board

- Research study recruitment messages do not require other administrative approvals
- Mailings to selected faculty, staff, and/or students

	1. Mailings directed at more than one audience must be approved by each responsible V.P., with the exception of IRB Approved recruitment messages. 2. Submit the fully approved request to ITS Mass Mail Service.
ITS Mass Mail Service Provider	1. Receive the "Request for Mass Electronic Mail." 2. Review for all necessary signatures. 3. Obtain University IDs of target population from requestor for staff and faculty, and from Registrar's office for students. (Note: For complex population requests, more than seven days may be required for processing.) 4. Submit test message for requestor approval. 5. Queue approved message for delivery. 6. Retain copy of approval.
Mail Recipient-Faculty, Staff	1. Set filters rules on your desktop mail client. 2. Review mail and respond to sender, if desired. If there appears to be any exception to this policy, send an e-mail note to its-email@ssiu.ac.in.
Mail Recipient - Student	1. Set e-mail preferences (filter rules) using the links on ISIS on the Web. 2. Review mail and respond to sender, if desired. If there appears to be any exception to this policy, send an e-mail note to its-email@ssiu.ac.in.

Policy Number: IT-10
Domain-name-policy

Description:

All hosts on the University network should have a name that ends in ssiu.ac.in. Hosts that do not must be approved by Telecommunication and Network Services (TNS) unit of Information Technology Services (ITS). Colleges or department technology representatives must register all hosts in the University of Iowa namespace.

The domain name system (DNS) is an Internet-wide distributed database of names primarily associated with Internet Protocol (IP) addresses. It is also a tool for locating services since many services are known by their domain name. For example, the hostname "www" has come to be well known as the name of a system which provides web (HTTP) service, and the domain name "www.ssiu.ac.in" is thus known as the primary web server address for The University of Iowa.

Definitions:

- The IP address is a 32-bit number, commonly represented as four 8-bit numbers separated by dots, used to identify a host on the Internet. The IP address is used by the network to route messages from one host to another. An example IP address on our campus network is 172.16.X.X
- Domain Name System (DNS) is the method or scheme for associating names with an IP address and other data. The domain name system is not an authentication system, or an authorization system. The use of DNS or IP addressing as the basis for authentication or authorization is discouraged. The practice of basing authentication or authorization on IP ranges is also discouraged. (This is commonly referred to as IP filtering.)
- DNS is also not a "white pages" directory. It contains information about computers and in some cases the services they provide. It does not reliably provide information about people.

Although an implied policy regarding the assignment of domain names has existed at the University of Iowa, there has been no formally agreed upon and approved policy. A formal policy is now necessary because:

- Individual departments and units within the University need to offer and communicate new or unique services to the Internet.
- There are an increasing number of requests for domain names that do not meet current DNS conventions.
- There have been requests for ITS TNS to register domain names outside the ssiu.ac.in domain.
- Domain names exist at the University of Iowa that are inconsistent with current naming conventions.

Policy Statement:

1. The principal domain name for the University of Iowa is "ssiu.ac.in". All services that are provided by members of the University of Iowa community as part of their official functions and as part of the mission of the institution will be registered within the ssiu.ac.in domain according to the Implementation Requirements attached to this policy.
2. All services that are provided by either members or nonmembers of the University of Iowa community, but that are not part of their official functions as members of the community or as part of the mission of the institution, must be registered outside the ssiu.ac.in domain according to the Implementation Requirements listed in this policy.
3. Services provided by University affiliates (e.g., UI Foundation) may be registered under the ssiu.ac.in domain, or may be registered outside of the ssiu.ac.in domain.
4. Services provided by University auxiliary units (UI Bookstore, UI Press, etc.) must be registered under the ssiu.ac.in domain.
5. Names outside of the ssiu.ac.in domain may be allowed if associated with the support of University-related organizations. For example, the University could provide DNS and web service for a pro bono basis scholarly journal, edited by a University faculty member.
6. All services listed outside the ssiu.ac.in domain must obtain their own IP address space. The network administrator must contact hostmaster@ssiu.ac.in to discuss associated domain name service and IP routing issues before requesting the domain name or configuring services related to the domain name or IP address space, unless otherwise arranged (such as per(5) above).
7. Existing hostnames or subdomains registered under ssiu.ac.in that do not conform to this policy will be reviewed to bring them into conformity with this policy, including the conditions for exceptions described below, or to grant them "grandfathered" status, if that is most appropriate.
8. All exceptions that are granted to the normal subdomain naming within the ssiu.ac.in domain will be assigned an alias to the domain that would otherwise normally apply to the request, if such a domain exists. This will allow users to use network tools to determine the unit to which a particular service is affiliated even though the affiliated unit does not appear in the exception name.

Implementation of the Policy:

1. Responsibility for implementing this policy will rest with the Telecommunication and Network Services (TNS) unit of Information Technology Services (ITS). To contact the TNS unit about domain name administration issues, send an electronic mail message to hostmaster@ssiu.ac.in.

2. Requests which are denied by the TNS unit may be appealed to the Campus CIO (Chief Information Officer).
3. If the justification for a non-standard domain name changes, the assignment of the name will be reviewed. For example, if grant funding ends and a center is no longer officially recognized, the domain name assignment will be reviewed.
4. If the domain name does not respond to network inquiry for two months, the assignment of the name may be terminated. Notice to the name owner will be given first, if possible.

Implementation Requirements:

DNS Standards Within the ssiu.ac.in Domain

The format of DNS service entries is "hostname.department.ssiu.ac.in", where:

1. The naming structure is intended to follow the organizational affiliation.
2. Department subdomains in the ssiu.ac.in domain must be the names of schools, colleges, or organizational units that are officially recognized by the University of Iowa. The subdomain name is determined by ITS and the department or college. For example, nursing.ssiu.ac.in.
3. The unit responsible for the computer may select the hostname component of the domain name.
4. The hostname component of the domain name may reflect generally accepted practices, used by the Internet-at-large and provided by sites internationally, including www and ftp. For example, the "www" in www.site.ssiu.ac.in
5. The hostname component of the domain name may reflect the name of the service program or may follow a naming scheme within the department. For example, the "gateway" in gateway.lib.ssiu.ac.in.
6. Length limit for hostname and department subdomain names is 63 characters each.
7. Server and computer hostnames should not be trademarked or copyrighted terms.
8. Server and computer hostnames must not be distasteful, obscene, or used to misrepresent their purpose.
9. Exceptions for hostnames within the ssiu.ac.in domain (e.g., wsui.ssiu.ac.in) may be allowed only if all of the following conditions are met:

- The proposed name is for a consortium of many different organizations either within or outside the University.
- The proposed name is the name of a service or service unit, center, or institute and not the name of a department or other organizational unit.
- The proposed name is for a University-wide service that is not easily identified with a single department or unit, or it is for a service that is being offered primarily to people or groups that are outside the University and who are not likely to be familiar with the details of the University's internal organizational structure.
- The proposed name is not now, and is not likely to become, ambiguous if it is used as a hostname without other department or unit qualification.
- The proposed name is not likely to change.
- The placement of the proposed name as a hostname within ssiu.ac.in has the explicit approval of the unit administrator of the school, college, institute, or unit with which the name would otherwise be associated.

DNS Requirements - Outside the ssiu.ac.in Domain

Domain names outside ssiu.ac.in may be allowed and may be required if all the following conditions are met. The proposed name should have either primary or secondary name service provided by ssiu.ac.in hosts.

The proposed name will be used by many people from many different organizations outside the University.
The proposed name is not likely to be confused with the name of a University of Iowa department or unit.
The proposed name signifies an organization or venture, commercial or noncommercial, that is not explicitly part of the University.
The proposed name is for a project with external funding.
The placement of the proposed name outside the ssiu.ac.in has the explicit approval of the university central administration or dean, director or departmental executive officer of the college, center, institute, or equivalent unit to which the name would otherwise be associated.

Related Policies, References and Attachments:

Swarrnim Startup & Innovation University ★ Gandhinagar

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE

INDIA'S FIRST UNIVERSITY FOR STARTUP

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.

They are incorporated into the University of Operations Manual http://opsmanual.ssiu.ac.in by reference, per the Policy on Acceptable Use of Information Technology Resources (opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

1. University of Iowa Policy on Web Publishing (under development)
2. Attachment 1: Implementation Requirements

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-12

University E-mail Address Policy

Description:

All users of the University must have a destination e-mail address and E-mail is sufficient written notice for "official" communication.

Purpose:

This policy provides for a required destination e-mail address for current students, faculty, staff and affiliates when they have established a recurring business-relationship with The University of Iowa. Former faculty, staff, and students are encouraged to maintain a destination address for continued communication with the institution.

This policy creates a standard method of e-mail communication to support reliable academic and administrative communication, designed to protect the options individuals have for selecting a destination e-mail address. The Enterprise Directory Service provides the necessary link between the known standard e-mail address and the mail routing or destination address.

Definitions:

University Standard E-mail Address: a standard-format e-mail address in the form of name.dept@ssiu.ac.in that can be used by anyone as a reliable form of address, regardless of the individual's destination e-mail address.

Mail Routing or Destination e-mail address: an accurate, up-to-date mailbox address at which an individual can be reached through e-mail. If an individual does not have one, an account will be provided through the ITS-Campus Services E-mail System. Only one destination address is allowed, at this time.

Complimentary Appointments (no pay appointment, i.e. 0% of time appointment): may elect to register a destination e-mail address but are not required to do so under this policy.

Enterprise Directory Service: The Enterprise Directory Service is an LDAP standards-based location for key personal and application attributes from authoritative institutional sources. The service makes institutional data and business rules accessible to campus service providers and provides the infrastructure for campus email routing.

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Statement:

1. This policy requires covered individuals to provide an accurate, current destination e-mail address for University-related academic and administrative transactions, unless exemption from so doing is allowable by law or business necessity.
2. This policy recognizes that compliance requires easy to use web methods for maintaining this destination address, specifically ISIS for students and ITS Directory and Account Management tools available from a variety of web links for faculty and staff.
3. The Enterprise Directory Service is the primary location of the link between the University Standard e-mail Address and the current destination e-mail address.
4. Where employment conditions, or work assignments require it, a supervisor may request that employees be exempt from this requirement. The request, which is to be in writing, must explain:

- why the employee, classification of employee(s) or workgroup should be exempt
- how such employees will be kept notified of University administrative mass e-mail communications e.g., a message from the UI President
- how such employees will be kept notified of University administrative targeted e-mail communications e.g., information from University Benefits to a specific list of employees

1. For the exemption to be granted, the request should go through normal administrative channels, including central Human Resources for staff and the Office of the Provost for faculty.
2. The University routinely uses email for both formal and informal communication with faculty, students and staff. All faculty, students, and staff are expected to check their email regularly for University communications. Official University communications include, but are not limited to, enrollment information, grade reports, financial statements and other financial information, library recall notices, and policy announcements.

Swarrnim Startup & Innovation University ★ Gandhinagar

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-15

EnterpriseAuthentication

Description:

Provides a fully integrated method for verifying the identity of all persons in the university community.

Authentication is the mechanism that verifies that an individual is who they claim to be. Verification is based on
1) something known (password);
2) something carried (smart card); or
3) something the individual is (biometrics).
The UI Enterprise Authentication infrastructure provides a fully integrated method for verifying the identity of all persons in the university community. As such, it is an enabler for institutional and collegiate services and is essential to campus IT security. Enterprise level directories – Enterprise Directory Services and Active Directory – provide the authentication infrastructure to improve the user and IT provider experience. Data in the authentication directory is fed from authoritative sources, making the data dependable and available for decisions. Central, uniform authentication makes the login process simpler for the user. It allows the provider to concentrate on the specifics of their service. Enterprise authentication offers opportunities for services beyond the campus boundaries where appropriate for student recruiting, patient care or alumni relationship services.

Definitions:

- Enterprise Authentication is the service defined herein.
  Enterprise Service is a service, such as e-mail or calendar, supported by any campus IT provider, that trusts the entire multi-domain enterprise authentication infrastructure as authentication for the service.Local Service is a service, supported by any campus IT provider, that authenticates its user base to a subset of domains in the forest, or to a local accounts database.Enterprise Directory Service (EDS) is an authoritative source for institutional data such as IDs, e-mail, service eligibility indicators, and other derived attributes. EDS consolidates identity information for support of enterprise authentication.Microsoft Active Directory (AD) is a directory that supports Windows services. AD is Microsoft's implementation of an LDAP directory with a number

enhancements for Kerberos support and workstation management.Campus Active Directory ssiu.ac.in Forest is the shared services forest, sponsored by a partnership of ITS and HCIS, that provides the infrastructure for campus Windows servers and workstations connected to the campus network. Active Directory is the current campus production authentication engine.Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. AD is a Kerberos implementation, with the boundaries of a domain providing the boundaries of a Kerberos realm. The terms Active Directory domain and Kerberos realm are synonymous in this context.SSIU ID is the campus-wide standard for a unique login identifier (ID) for each person in the UI community. This SSIU ID, therefore, is the account ID used in the enterprise authentication service.SSIU ID Password is the password associated with the SSIU ID in the enterprise authentication service.
Local Service ID is the service-specific login ID for a service not yet enabled to use enterprise authentication. Service providers are encouraged to use the SSIU ID as this local service ID. Local Service Password is the service-specific password for a locally-authenticated service. If there are security issues in the local service, such as use of clear-text passwords, the local service password should not be synchronized with the SSIU ID password.

Policy Statement:

The Enterprise Authentication infrastructure provides a fully integrated method for verifying the electronic identity of all persons in the university community. As such, it is an enabler for institutional and collegiate services and is essential to campus IT security.

Developed through an enterprise-wide initiative, the Campus Active Directory Forest provides the account database for the production authentication service. The use of the forest for enterprise authentication is native for AD-enabled services. There are several available authentication protocols, such as NTLM, Kerberos, Radius, or LDAP, that can be used to traverse the multiple forest domains.

The fundamental underlying premise to the Enterprise Authentication Service is that there is a single unique account ID per person in the forest. That is, a person's SSIU ID will appear in one and only one domain in the forest. This guarantees the uniqueness of the enterprise SSIU ID and SSIU ID password pair. And, in accordance with the "Enterprise Login ID Standard" policy, the account IDs in all domains of the Campus Forest will be maintained in sync with the Enterprise Directory SSIU ID assignment.

Swarrnim Startup & Innovation University Gandhinagar

Swarrnim Startup & Innovation University Bhoyan Rathod, Gandhinagar

The domain administrators of each domain in the forest are committed to maintaining accounts for the persons for whom they have responsibility, in support of the enterprise authentication requirements identified by campus IT service providers.
Services using enterprise authentication are responsible for the longevity of the SSIU ID.

Enterprise Directory Service:

The Enterprise Directory Service is the authoritative source for assignment and maintenance of SSIU IDs used in deployment of campus services. As a repository for key personal and application attributes from authoritative institutional sources, the directory service acts as a centralized accessible source of business rules that determine institutional roles. Domain assignments are based on current roles.

SSIU ID and SSIU ID Password:

The **SSIU ID** is the account ID used in the enterprise authentication service. The associated password is the **SSIU ID Password.**
For service environments that are not able to fully utilize the enterprise authentication service, the IT provider is encouraged to use the SSIU ID as the service login ID. The associated password should be referred to as a service-specific password.

Non-Windows (Kerberos Realm) Authentication:

When multiple domain authentication is not possible, an Active Directory Kerberos Realm can provide the authentication account base for non-Windows-based services. IT providers utilizing single-domain authentication should select the domain that best supports their service user base. If all users are not in a single domain, local authentication must be used in conjunction with the Kerberos Realm authentication.

Local Authentication :

Services that cannot use multiple-domain or Kerberos authentication must rely on local authentication until such time as the service can use Active Directory based authentication.

Clear-Text and Encrypted Passwords:

The enterprise authentication service is intended for use by campus services that provide encrypted password streams. Legacy applications that use clear-text passwords should be evaluated for risk. Service owners for systems and applications using clear text passwords sho

consider upgrades that include encrypted passwords.
Service owners are responsible for educating their users of the importance of protecting their enterprise password by using an alternate password, if possible, for these services that are not integrated and which send clear-text passwords.

Future Campus Software Acquisitions, Development:

Future software deployments must include these considerations:

1. Support for secure authentication.
2. Interoperability with Active Directory.
3. Support for login IDs consistent with the "Enterprise Login ID Standard."

Resource or Service ID Authentication:

Local domain resource or service IDs, such as IDs created for applications, testing, or for departmental or generic use IDs typically assigned as web site and e-mail service IDs, may exist in Active Directory without a corresponding entry in the Enterprise Directory Service.

Resource IDs that are used to authenticate to enterprise services must not collide with existing SSIU IDs, and therefore must be registered within the Enterprise Directory Service. Domain specific test IDs with local impact only, should be created in accordance with the service ID naming conventions. (See "Enterprise Login ID Standard".)

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of ssiu policy.They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

1. Enterprise Active Directory Policy

Swarrnim Startup & Innovation University Gandhinagar

2. Enterprise Password Policy
3. Enterprise Login ID Standard
4. Domain Assignment / Active Directory Account Management

Nothing in this policy is intended to be in violation of FERPA or HIPPA requirements

Swarrnim Startup & Innovation University Bhoyan Rathod, Gandhinagar

Swarrnim Startup & Innovation University Gandhinagar

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-16

Policy-roles-and-responsibilities

Description:

To define the roles and responsibilities of the University community who are responsible for information assets and security at the University of Iowa.

Policy Statement:

The University of Iowa is responsible for implementing a comprehensive enterprise information security program. This responsibility is delegated to the following groups and individuals:

- University Level Roles: Data Steward
  Information Security Committee
  Chief Information Security Officer
  Unit Level Roles: Business Owner
  Department Security Liaison
  Data Custodian
  Authorized User

Data Steward:

The enterprise vice-president or top-level executive having policy-level responsibility for a particular set of information assets. The Data Steward will:

1. Establish standards for business use of information.
2. Assign administrative responsibility to Business Owners.
3. Monitor compliance and periodically review violation reports.

Information Security Committee (ISC):

The Information Security Committee is responsible for governance and oversight of the enterprise information security program. The ISC will:

Perform all responsibilities of Data Custodian when placing institutional data on personally owned or managed devices.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://www.ssiu.ac.in/~our/opmanual/index.html) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

Backup and Recovery Policy
Computer Data and Media Disposal Policy
Information Security Framework Policy
Institutional Data Access Policy
IT Security Incident Escalation Policy

1. Analyze and manage institutional risks.
2. Review and recommend policies, procedures, and standards.
3. Ensure consistency in disciplinary processes for violation.

Chief Information Security Officer:

The official responsible for directing implementation of the enterprise information security program. The Chief Information Security Officer will:

1. Coordinate the development and maintenance of information security policies and standards.
2. Investigate security incidents and coordinate their resolution as defined in the IT Security Incident Escalation Policy.
3. Assist Business Owners in assessing their data for classification as defined in the Institutional Data Access Policy and advise them of available controls.
4. Implement an information security awareness program.
5. Serve as liaison to the Information Security Committee, law enforcement, Internal Audit, and University Legal Services.
6. Provide consulting services for information security throughout the enterprise.

Business Owner The senior official within a college or departmental unit (or his/her designee) accountable for managing information assets. The Business Owner will:

Approve business use of information.
Identify Data Custodian(s) (see below) for each segment of information under his/her control.

Ensure implementation of policies, and documentation of process and procedures for guaranteeing availability of systems, including:

- Risk assessment
- Disaster recovery
- Operating in an emergency
- Software testing and revision controls

1. Determine security classification of each segment of data as described in the Institutional Data Access Policy.

2. Define departmental access roles and assign access for individuals based on their need to know.
3. Ensure that all department/unit personnel with access to information assets are trained in relevant security and confidentiality policies and procedures.
4. Ensure the protection of health information assets under his/her control, including:

- Register all health information assets containing individually identifiable health information (e.g., Protected Health Information, or "PHI") in any medium with the University HIPAA Privacy Officer.
- Ensure that validated corrections to health information are implemented.
- Ensure compliance with federal and state laws and University policy regarding the use of individually identifiable health information in directed communication/solicitation.
- Require the completion of an information sharing agreement before access to health information assets is granted to external entities.

Network Security Contact (NSC):

The individual within a department/unit who acts as a liaison for timely and relevant information flow between central networking and IT security personnel and the department/unit.

The NSC will:

Receive all security vulnerability reports for departmental/unit computer systems and disseminate such information to appropriate technical staff for resolution. Receive network alerts, outage notifications, or other networking issues affecting the department/unit and disseminate such information to appropriate staff. Coordinate departmental response to computer security incidents.

Data Custodian:

The technical contact(s) that have operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of computer hardware and software platforms. The data custodian may or may not be IT staff. The Data Custodian will:

Define and implement processes for assigning User access, revoking User access privileges, and setting file protection parameters.
Implement data protection and access controls conforming to the Institutional Data Access

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-17
policy-backup-recovery

Description:

Minimum requirements for the creation and retention of computer data backups.

All electronic information which is a "UI record" as defined in the University Operations Manual Chapter 17.3 Records Management Program (hereafter referred as UI records for the purpose of this policy) must be copied onto secure storage media on a regular basis (i.e., backed up), for the purpose of disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, should be accommodated on an individual basis.

Scope:

Data custodians are responsible for providing adequate backups to ensure the recovery of electronic information (includes UI Records and software) in the event of failure. These backup provisions will allow University business processes, including the research enterprise to be resumed in a reasonable amount of time with minimal loss of data. Since failures can take many forms, and may occur over time, multiple generations of backups should be maintained. Federal and state regulations pertaining to the long-term retention of information (e.g., financial records) will be met using separate archive policy and procedures, as determined by the Business Owner of the information, and in accord with the Records Management Program. Long-term archive requirements are beyond the scope of this policy.

Policy Statement:

- Backups of all UI records and software must be retained such that computer operating systems and applications are fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
- The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data. At a minimum, backup copies must be retained for 30 days.
- At least three versions of UI Records must be maintained.
- At a minimum, one fully recoverable version of all UI Records must be stored in a secure, off-site location. An off-site location may be in a secure space in a separate University building, or with an off-site storage vendor approved by the Information Security and

Policy, Information Security Framework Policy, and the Computer Data and Media Disposal Policy.
Define and implement procedures for backup and recovery of information as defined in the Backup and Recovery Policy.
Ensure processes are in place for the detection of security violations.
Monitor compliance with information security policy and standards.
Limit physical access to information assets, including:

Equipment control (inventory and maintenance records), and physical security of equipment (locks, HVAC).
Authorization procedures prior to physical access to restricted areas, such as data centers, with sign-in or escort of visitors, as appropriate.

Implement a system for software change management and revision controls.
Maintain ongoing internal audit processes (to the extent technologically practical), which record system activity such as log-ins, file accesses, and security incidents.
Maintain records of those granted physical access to restricted areas (i.e., key card access lists).

Provide special handling and physical protection for health information assets, including:

Operating and maintenance personnel are given access only as necessary to perform system maintenance responsibilities. Authorized persons supervise all external personnel performing maintenance activities.

Authorized User:

Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users include, but are not limited to faculty and staff members, trainees, students, vendors, volunteers, contractors, or other affiliates of the University of Iowa. Users will:

Seek access to data only through the authorization and access control process.
Access only that data which s/he has a need to know to carry out job responsibilities.
Disseminate data to others only when authorized by the Business Owner.
Report access privileges inappropriate to job duties to the Business Owner for correction.
Attend training in security and confidentiality policies/procedures.
Access to Level III data must be individually authorized by the Business Owner and an annual confidentiality agreement must be acknowledged or signed by all authorized users.

Swarrnim Startup & Innovation University Gandhinagar

Policy Office. The practice of taking backup media to the personal residence of staff persons is not acceptable. (See Appendix A for a list of approved off-site storage facilities.)

- Derived data should be backed up only if restoration is more efficient than creation in the event of failure.
- All UI Record information accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to allow for backup. UI Record information located directly on workstations, laptops, or other portable devices should be backed up to networked file server drives. Alternatively, UI Record information located directly on workstations, laptops, or other portable devices may be backed up using a 3rd party vendor approved by the Information Security and Policy Office. (See Appendix A for a list of approved desktop backup services.) Convenience records and Non-records, or other information which does not constitute a UI Record does not carry this requirement.
- Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.
- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- Recovery procedures must be tested on an annual basis.

Related Policies, References and Attachments:

University Operations Manual, Records Management Program (Chapter 17.3)
Roles and Responsibilities for Information Security
Institutional Data Access Policy
How to register your system(s) in the Uiowa System Registry (USR)
Disaster Recovery and Business Continuity Planning

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.

They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in/) by reference, per the Policy on Acceptable Use of Information Technology Resources

(http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

Appendix A: Approved Facilities and Services:

Off Site Storage Facilities: Advantage Records Management & Storage (any UI system) (http://www.advantagerms.com)
Desktop Backup Services: Departmental File Servers Connected (Iron Mountain, Inc.)

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-18

Policy-Information-Security-Framework

Description:

The purpose of this policy is to identify and disseminate the University of Iowa's framework and principles that guide institutional actions and operations in generating, protecting, and sharing confidential information.

Information assets of the University of Iowa, in all its forms and throughout its life cycle, will be protected through information management policies and actions that meet applicable federal, state, regulatory, or contractual requirements and support the University of Iowa's mission, vision, and values. The purpose of this policy is to identify and disseminate the University of Iowa's framework and principles that guide institutional actions and operations in generating, protecting, and sharing institutional data.

Scope:

This policy applies to all institutional data owned by The University of Iowa. The Institutional Data Access Policy defines three sensitivity levels (low, moderate, and high) which categorize institutional data. Each faculty and staff member, trainee, student, vendor, volunteer, contractor, or other affiliate of the University of Iowa with access to institutional data is subject to and has responsibilities under this policy.

Principles:

- Access to University of Iowa Level II and Level III data may only be granted to Authorized Users on a need-to-know basis. The Business Owner of the data as defined in the Roles and Responsibilities for Information Security policy must approve and verify such access.
- All Authorized Users shall receive education on the expectations, knowledge, and skills related to information security.
- Every user must maintain the confidentiality of Level II & III institutional data even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.
- If an Authorized User elects to place institutional data onto personally owned or University owned and personally managed media, laptops, USB keys, or storage devices or maintains a personal database, s/he is responsible for ensuring that its security, confidentiality, and integrity are maintained in accord with this policy.

Swarrnim Startup & Innovation University Bhoyan Rathod, Gandhinagar

- The User is personally responsible for any breaches that occur as a result of his/her actions.
- A Data Custodian must be identified by the Business Owner for all institutional data as defined in the Roles and Responsibilities for Information Security policy. A Data Custodian is the person responsible for capture, maintenance, protection, and dissemination of institutional data.
- Everyone has an obligation to report instances of non-compliance to the Chief Information Security Officer.
- Users who access data for which they do not have a need to know and/or commit breaches of confidentiality may be subject to disciplinary action up to and including discharge, termination of contract/relationship, and/or liability to civil and criminal penalties.
- Everyone must comply with all applicable industry standards, federal, and state regulations and controls (e.g., PCI-DSS, FERPA, HIPAA, GLBA, FISMA etc.) governing the access and use of data.

Swarrnim Startup & Innovation University Bhoyan Rathod, Gandhinagar

Roles:

Responsibility for The University of Iowa's comprehensive enterprise information security program is delegated to the groups and individuals as defined in the Roles and Responsibilities for Information Security Policy.

Information Assessment and Classification:

Business Owners will assess risks and threats to data for which they are responsible, and accordingly classify and oversee appropriate protection of institutional data as described in the Institutional Data Access Policy.

Information Access :

Physical and electronic access to institutional data must be controlled. The level of control will depend on the classification of the data and the level of risk associated with loss or compromise of the information. Data handling requirements are outlined in the Institutional Data Access Policy.

Physical Access Control :

Swarrnim Startup & Innovation University Gandhinagar

- All devices with Level II & III institutional data and all mobile devices must be kept in a physically secure (locked) location when staff are not present.
- The level of physical access control for any area that contains institutional data is determined by the level of risk and exposure. Data centers and other locations where Level II & III data is housed must be protected at all times by physical access controls such as keys, biometrics or proximity cards.
- Physical access to data centers or any area with Level III data must be monitored and logged through electronic logging or tracking mechanism. Visitors and other maintenance personnel must be escorted by authorized operations staff when in a data center.
- Media (e.g., paper records, digital devices and peripherals) that contains Level III data must be secured during transportation and disposal.

Electronic Access Control:

Access control will be regulated by the following University of Iowa Policies: University Login ID Standard, Enterprise Authentication, and the Enterprise Password Policy.

In addition,

- For Level II & III data, criteria must be established by the Business Owner for account eligibility, creation, maintenance, and expiration.
- Access to Level III data must be individually authorized by the Business Owner and an annual confidentiality agreement must be acknowledged or signed by all authorized users.
- Data Custodians must periodically review user privileges and modify, remove, or inactivate accounts when access is no longer required.
- Procedures must be documented for the timely revocation of access privileges and return of institutionally owned materials (e.g., keys, ID Cards), for terminated employees and contractors.
- Inactivity time-outs must be implemented, where technically feasible, for workstations that access Level III data. The period of inactivity shall be no longer than 20 minutes in publicly accessible areas.

Secondary Use

An authorized user of Level I & II data may re purpose the information for another reason or a new application when it is authorized by the Business Owner. Secondary use or re purposing of Level III data is prohibited.

External Data Sharing

Level II & III data will be shared outside the University of Iowa as allowed by Iowa Open Records Law, FERPA restrictions, or Non-UI Project or study participants. Level III data, specifically Protected Health Information (PHI) will only be shared based on HIPAA Business Associate Agreements.

Access to Data for Automated Operations (Generic, Scheduled, or Task Initiated Access)

Generic access to information stored in databases is allowed only for non-interactive tasks. A non-interactive task is one that is scheduled to run automatically or one that is triggered by a series of events. It is automatically initiated, and the output is automatically handled by software. This includes automatic downloads and other linkages for data transfer.

- Requests for generic access to information stored in databases for automated operations are made to the Business Owner, and if approved, will be executed by the Data Custodian.
- Generic account passwords must be protected from unauthorized disclosure. Hard coded passwords that reside on a client machine or in an application must be reasonably protected (i.e. encrypted), commensurate with risk and the available platform or application security features.
- Information access via generic accounts must be limited to the specific task required.

Systems administered by contractors

An on-site Data Custodian must be identified to oversee administrative duties performed by contractors to ensure their compliance with security policies and standards. Contractor activities will be controlled and monitored as follows:

- Contractor user accounts must not allow more system or network privileges than necessary to meet contract requirements.
- Secure authentication of contractors is required.
- Logging and auditing of system accesses and activity is required.
- Contractors will be required to sign a confidentiality agreement before handling any Level II or III institutional data.

Swarrnim Startup & Innovation University Gandhinagar

Audits

- Data Custodians must be able to audit logins to Level II institutional data, and logins, accesses, and changes to Level III institutional data.
- Audit log records shall be kept a minimum of three months, or as defined by specific regulations pertaining to the data. The Business Owner and/or Data Custodian shall periodically review the audit records for evidence of violations or system misuse. An investigation must be conducted if unauthorized access, login, or changes are identified.
- All authorized users shall be notified that access, login, and change audits will be conducted for Level III institutional data. If evidence of improper data access is discovered, it may result in disciplinary action.
- The location of computer systems containing Level III institutional data, including but not limited to Social Security Numbers, Credit Card Numbers, and Protected Health Information, must be registered with the Information Security and Policy Office. (see how to register your system by clicking the USR link in Related Policies, References and Attachments section below.)

Communication Security

Institutional data transmitted outside the organization requires additional safeguards. The security provisions employed will depend upon the identified risk and threats, regulatory requirements, and the technical mechanisms available.

- The Business Owner is responsible for making decisions regarding appropriateness of external transmission and access to institutional data.
- Externally sharing PHI requires the completion of a HIPAA Business Associate Agreement unless the communication is authorized for the purpose of treatment, payment or health care operations.
- The Chief Information Security Officer will review and approve technical security mechanisms and services for remote access and external transmission of Level III institutional data.
- External network transmission and exchange of Level III institutional data over open networks such as the Internet or outside of the UI managed network must be encrypted and include strong authentication.
- Encryption must be employed for all external transmissions of Level III institutional information via electronic mail, except as authorized by the subject of the data.
- University owned mobile devices (examples include laptops, tablets and external storage devices) must utilize full disk encryption.

Information Integrity Controls

Information must remain consistent, complete and accurate. Integrity errors and unauthorized or inappropriate duplications, omissions and intentional alterations will be investigated and reported to the Business Owner of the affected data.

Separation of duties and functions

Tasks involved in critical business processes must be performed by separate individuals. Responsibilities of programmers, system administrators and database administrators must not overlap, unless authorized by the Business Owner of the data.

Systems and Application software

- System and application software must be tested before installation in a production environment.
- System and application software must be protected from unauthorized changes.
- All security updates must be applied in a timely manner, commensurate with the risk associated with the addressed vulnerability.

Change controls

A system for change control management must be implemented for systems handling Level II & III institutional data, to monitor and control hardware and software configuration changes. Change control includes documentation of change requests, approvals, testing, and final implementation.

Anti-Malware controls

- All systems connected to the network will have virus protection where technologically feasible.
- The most recent version of anti-virus software must be implemented and maintained with daily virus signature/pattern updates

Preventive Measures, Backup and Recovery

Processes are necessary to prevent loss of vital information, to provide backup and recovery, and provide continuous operation consistent with the business needs of the institution.

- **Prevention:** Annual testing of preventive methods as they apply to fire, utility services and other environmental hazards must occur.
- **Backup:** All information must have sufficient backup and be fully recoverable. Responsibilities are described for the regular backup and safe recovery of systems in the Backup and Recovery Policy.
- **Emergency Mode of Operation:** Alternate modes of operation, that may include manual methods, must be documented to ensure continuity of critical services in the event a natural disaster, fire, act of vandalism, or act of terrorism occurs.
- **Disaster Recovery Planning:** All data centers and computerized systems critical to the University of Iowa must have written and tested disaster recovery plans. Business Owners will prioritize the recovery of applications and associated databases to ensure critical services are recoverable in a timely fashion.

Mobile Device Security

Mobile devices present a unique challenge to securing sensitive data. Lost or stolen devices must be protected from unauthorized access and sensitive data disclosure.

- Mobile devices containing institutional data must be kept in a secure location when not in use, and the device must be access controlled with a password.
- Full disk encryption is required for university-owned mobile client devices (e.g. laptops, tablets) unless the device meets criteria for an exception. Personally-owned mobile devices must employ full disk encryption if Level III (highly sensitive) institutional data is authorized to be stored locally.
- Employees must use University provided storage services (such as OneDrive) rather than externally attached storage devices (such as USB flash drives) whenever possible, to minimize the risk of lost or stolen devices and institutional data.
- Departments that routinely handle Level III data:
    - All external storage devices must be encrypted prior to writing institutional data
    - Ability to write data to an external storage device will be restricted to authorized computers

- All client computers (desktop and mobile) will utilize full disk encryption
- Departments that do not routinely handle Level III data:
  - External storage devices must be encrypted prior to writing Level III institutional data
  - Client computers (desktop and mobile) are recommended to utilize full disk encryption

Data Disposal:

Proper data disposal is essential to controlling sensitive data. Media or devices containing sensitive information that are transferred between departments or are removed from service must be properly erased, as described in the Computer Data and Media Disposal Policy.

- Devices containing Level II data must be wiped or erased.
- Devices containing Level III data must be DOD-level wiped or have the media destroyed before disposal.
- Printed reports with Level II data should be recycled, and reports with Level III data must be shredded.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Ä̈cceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

Backup and Recovery Policy
Computer Data and Media Disposal Policy
Enterprise Authentication
Enterprise Password
Institutional Data Access
Roles and Responsibilities for Information Security
University Login ID Standard
Encryption Resources

How to register your system(s) in the Uiowa System Registry (USR)
IT Security and Network Log Retention Guidelines

Policy Number: IT-19

Policy-Institutional Data Access

Description:

To establish policy for the classification and use of University institutional data and the responsibilities for the protection of such data.
Institutional data is information that supports the mission and operation of The University of Iowa. It is a vital asset and is owned by the University. It is likely that some institutional data will be distributed across multiple units of the University, as well as entities outside.
Institutional data is considered essential, and its quality must be ensured to comply with legal, regulatory, and administrative requirements. Business Owners (as defined in the Roles and Responsibilities for Information Security Policy) will assess institutional risks and threats to the data for which they are responsible, and accordingly classify its relative sensitivity as Level I (low sensitivity), Level II (moderate sensitivity), or Level III (high sensitivity). Unless otherwise classified, institutional data is Level II. University personnel may not broaden access to institutional data without authorization from the Business Owner. This limitation applies to all means of copying, replicating, or otherwise propagating institutional data.

Data Classification

Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality (need for privacy), but also the need for integrity and availability. The need for integrity, or trustworthiness, of institutional data should be considered and aligned with institutional risk; that is, what is the impact on the institution should the data not be trustworthy? Finally, the need for availability relates to the impact on the institution's ability to function should the data not be available for some period of time. There are three classification levels of relative sensitivity which apply to institutional

data:

Level I: Low Sensitivity:

Access to Level I institutional data may be granted to any requester, or it is published with no restrictions. Public data is not considered sensitive. The integrity of "Public" data should be protected, and the appropriate Business Owner must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should Level I data not be available is typically low, (inconvenient but not debilitating). Examples of Level I "Public" data include published "white pages" directory information, maps, departmental websites, and academic course descriptions.

Level II: Moderate Sensitivity:

Access to Level II institutional data must be requested from, and authorized by, the Business Owner who is responsible for the data. Access to internal data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's employing unit or affiliation. Non-Public or Internal data is moderately sensitive in nature. Often, Level II data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the institution should this information not be available when needed is typically moderate. Examples of Level II "Non-Public/Internal" institutional data include project information, official university records such as financial reports, human resources information, some research data, unofficial student records, and budget information.

Level III: High Sensitivity:

Access to Level III institutional data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job, or to those individuals permitted by law. Access to confidential/restricted data must be individually requested and then authorized by the Business Owner who is responsible for the data. Level III data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of Level III "Confidential/Restricted" data include official student grades and financial aid data; social security and credit card numbers; individuals' health information, and human subjects research data that identifies an individual.

To comply with federal Health Insurance Portability and Accountability Act (HIPAA) regulations, the location of all Protected Health Information ("PHI") must be registered with the University's HIPAA Privacy Officer. (PHI includes any health information that pertains to an individual.) Contractual "Business Associate Agreements" may be required to share PHI with external entities.

Policy Statement:

- Institutional data must be protected from unauthorized modification, destruction, or disclosure. Permission to access institutional data will be granted to all eligible University employees for legitimate university purposes.
- Authorization for access to Level II and Level III institutional data comes from the Business Owner, and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other authority.
- Where access to Level II and Level III institutional data has been authorized, use of such data shall be limited to the purpose for which access to the data was granted.
- University employees must report instances in which institutional data is at risk of unauthorized modification, disclosure, or destruction.
- Business Owners must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with University policy and procedure.
- Business Owners must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.
- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Data Handling Requirements:

	LEVEL I Low Sensitivity (Public Data)	LEVEL II Moderate Sensitivity (Non- Public/Internal Data)	LEVEL III High Sensitivity (Confidential/Restricted Data)

Mailing & Labels on Printed Reports	None	May be sent via Campus Mail; No labels required	Must be sent via Confidential envelope; Reports must be marked "Confidential"
Electronic Access	No controls	Role-based authorization	Individually authorized, with a confidentiality agreement
Secondary Use (re-purposing data)	As authorized by Business Owner	As authorized by Business Owner	Prohibited
Physical Data/Media Storage	No special controls	Access Controlled area	Access controlled and monitored area
External Data Sharing	No special controls	As allowed by Iowa Open Records Law, FERPA restrictions; or Non-UI project/study participants	As allowed by Federal regulations; Iowa Open Records Law; FERPA restrictions; and Business Associate Agreement (for PHI);
Electronic Communication	No special controls	Encryption recommended for external transmission	Encryption required for external transmission
Data Tracking	None	None	Social Security Numbers, Credit Cards, and PHI locations must be registered
Data Disposal	No controls	Recycle reports; Wipe/erase media	Shred reports; DOD-Level Wipe or destruction of electronic media
Auditing	No controls	Logins	Logins, accesses and changes

Mobile DevicesUniversity-owned	Password protected; Secure storage when not in use; Full disk encryption required (unless granted an exception).	Password protected; Secure storage when not in use; Full disk encryption required (unless granted an exception).	Password protected; Locked when not in use; Full Disk Encryption required, no exceptions are allowed.
Mobile Devices - User-owned	Password protection and secure storage is recommended.	Password protected; Secured when not in use, full disk encryption recommended.	Password protected, secured when not in use, full disk encryption required.

Control Definitions:

Mailing & Labels on Printed Reports – A requirement for the heading on a printed report to contain a label indicating that the information is confidential, and/or a cover page indicating the information is confidential is affixed to reports.

Electronic Access – How authorizations to information in each classification are granted.

Secondary Use – Indicates whether an authorized user of the information may repurpose the information for another reason or for a new application.

Physical Data/Media Storage – The protections required for storage of physical media that contains the information. This includes, but is not limited to workstations, servers, storage devices, media, and mobile devices.

External Data Sharing – Restrictions on appropriate sharing of the information outside of the University of Iowa

Electronic Communication – Requirements for the protection of data as transmitted over telecommunication and data networks.

Data Tracking – Requirements to centrally report the location (storage and use) of information with particular privacy considerations.

Data Disposal - Requirements for the proper destruction or erasure of information when decommissioned (transfer or surplus), as outlined in the University's Computer Data and Media Disposal Policy.

Auditing – Requirements for recording and preserving information accesses and/or changes, and who makes them.

Mobile Devices – Requirements for the protection of information stored locally on mobile devices. This includes, but is not limited to laptops, tablets, and external storage devices that are university owned, as well as for personal devices that are utilized to store institutional data.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.

They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in/) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

Computer Data and Media Disposal Policy
Information Security Framework Policy
Roles and Responsibilities for Information Security
Backup and Recovery Policy
Social Security Numbers Policy
Data Classification Guidelines
Records Management Program
Encryption Resources
How to register your system(s) in the Uiowa System Registry (USR)
Iowa Regents Institutions Security and Network Log Retention Guidelines

Policy Number: IT-20

Airspace

Description:

In order to minimize potential interference with University of Iowa wireless services, the University must remove sources of interference when possible. This will assure the highest level of service for all members of the U of I campus community. This policy asserts the right of the University to remove devices using publicly unlicensed bands that cause interference with University services.

The University of Iowa's wireless data networking service allows authorized users to access computing resources from mobile computing devices via radio waves in the ISM and UNII bands. In order to ensure the success of this service, the University of Iowa needs the cooperation of all

of its community members in minimizing the number of devices that can cause interference and service disruption.

Scope:

This policy affects any device located on University-owned or University-rented property utilizing the ISM or UNII bands.

Policy Statement:-

Information Technology Services (ITS) department of the University reserves the right to restrict the use of all 2.4 GHz and 5 GHz radio devices in University-owned buildings, University-rented spaces, and all outdoor spaces on the University of Iowa campus. This may require the removal of equipment not sanctioned by ITS, including (but not limited to) some devices of the following types: cordless telephones, wireless microphones, wireless cameras, and network access points. Appendix A lists wireless devices that are currently banned on campus. ITS will work with faculty and staff to accommodate the use of devices for reasonable applications, such that they do not interfere with University delivered services, when possible. If you would like to use devices that utilize 2.4 GHz or 5 GHz radio frequencies, you must first contact ITS via email at ITS-NetworkServices@ssiu.ac.in or the Help Desk at 4-4357, so an impact assessment can be made.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources).

1. Wireless Network Standards
2. Appendix A – Banned ISM/UNII devices:
   Apple AirPort Base Station
   Apple Airport Extreme Base Station
   Netgear ME-102

Policy Number: IT-21
Computer Equipment Disposal

Description:

University of Iowa policy regarding the proper transfer, disposal and/or reuse of computers and other digital storage media.

Digital storage devices which contain licensed software programs and/or institutional data must be reliably erased and/or destroyed before the device is transferred out of University control or erased before being transferred from one University department or individual to another. The University of Iowa is committed to compliance with federal statutes associated with the protection of confidential information as well as ensuring compliance with software licensing agreements.

Introduction:

Digital storage devices which contain licensed software programs and/or institutional data must be reliably erased and/or destroyed before the device is transferred out of University control or erased before being transferred from one University department or individual to another. The University of Iowa is committed to compliance with federal statutes associated with the protection of confidential information as well as ensuring compliance with software licensing agreements.

Scope:

All constituents of The University of Iowa have a responsibility to ensure the confidentiality of federally regulated and otherwise protected sensitive or proprietary information residing on University-owned computer systems and other digital storage devices and media.All computers and digital storage devices including, but not limited to desktop workstation, laptop, server, notebook, and handheld computer hard drives; external hard drives; and all external data

storage devices such as disks, SANs, optical media (e.g., DVD, CD), magnetic media (e.g., tapes, diskettes), and non-volatile electronic media (e.g., memory sticks), are covered under the provisions of this policy.

Policy Statement:

1. University-owned computer and digital storage media must have all institutional data and licensed software reliably erased from the device prior to its transfer out of University control, and/or the media must be destroyed, using current best practices for the type of media. Delete, Remove, and Format operating system commands, as well as disconnecting or clipping wires to a drive, do *not* actually erase data from the media, and therefore are not acceptable methods for preparing media for transfer or disposal.
2. All computer and digital storage media leaving the University's possession and/or control while still intact must be transferred in accordance with the University of Iowa Equipment policy (Operations Manual Part V, Chapter 12), which covers both tagged and non-tagged equipment.University Surplus will request documentation attesting to the erasure of licensed software and institutional data by an approved IT service provider. Otherwise, they will either perform the erasure of data according to approved procedures prior to release (e.g., sale, donation) of the computer or digital storage media or they will be responsible to destroy the media.
3. Departments may be approved to erase computer and digital storage media for transfer within the University, and/or to destroy media, using approved best practices developed by the University Information Security & Policy Office (ISPO). The University ISPO will work with the appropriate department IT staff to ensure that procedures consistent with security best practices are followed for the reliable removal of licensed software and confidential data before equipment transfers take place. Otherwise, departments must engage a campus IT service provider approved by the ISPO to prepare media for transfer or disposal.
4. Computer and electronic storage equipment identified for title transfer must be reviewed and then subsequently cleaned by an IT service provider approved to perform data erasing. Licensed software and institutional data deemed to be the property of the University of Iowa must be removed prior to title transfer of equipment from the University.
5. Computer and digital storage media which are included as part of a trade-in purchase must be identified on the purchase order for new equipment.Documentation attesting to the erasure of licensed software and institutional data by an approved IT service provider will be required in order to complete the purchase. The University must have a confidentiality agreement in place with any vendor receiving devices for trade-in, or that must be replaced as part of a warranty or repair contract but which can not be erased for technical reasons.

Related Policies, References and Attachments:

The collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
Information technology policies are incorporated into the University of Iowa Operations Manual (available online at http://opsmanual.ssiu.ac.in), through the Policy on Acceptable Use of Information Technology Resources (see http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources).
All Information technology policies are available at http://itsecurity.ssiu.ac.in/university-it-policy. Best practices documents are available at http://itsecurity.ssiu.ac.in/resources/

Specific policies, procedures, and practices related to this policy are:

Information Security Framework Policy
Institutional Data Access Policy
Best Practices for Securely Removing Data from Computers and Electronic Storage Devices
Research Data Policy (under development)

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-23

Computer Security Breach Notification Policy

Description:

To define the circumstances under which the University shall provide notice to individuals regarding a breach in security of private information. The University of Iowa shall provide timely and appropriate notice to affected individuals when there is reasonable belief that a breach in the security of private information has occurred. A breach in security is defined as an unauthorized acquisition of information, typically maintained in an electronic format by the University.

Scope:

Attacks on University IT resources are infractions of the Acceptable Use Policy constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on University systems and/or on University networks to appropriate authorities is a requirement of all persons affiliated with the University in any capacity, including staff, students, faculty, contractors, visitors, and alumni.

Policy Statement:

Suspected or confirmed information security breaches must be reported to University authorities. This includes the affected management or collegiate unit officer, as well as the Information Security and Policy Office (ISPO). Contact the ISPO by sending a message to it-security@ssiu.ac.in or calling 319-335-6332.

The ISPO will investigate the report, and if a security breach of private and/or highly sensitive information may have occurred, will inform the Chief Information Officer (CIO) and/or law enforcement, as appropriate.

In the event that a public notification of the security breach may be warranted, the CIO will consult with the appropriate University Vice President(s), Provost, and General Counsel to develop the response and make the final determination if a public notification of the event is warranted.

Procedures:

The entity responsible for support of the system or network under attack is expected to:

1. Report the attack to their management and to the ISPO
2. Block or prevent escalation of the attack, if possible
3. Follow instructions communicated from the ISPO in subsequent investigation of the incident and preservation of evidence
4. Implement recommendations from the ISPO
5. Repair the resultant damage to the system

Internal Notifications

The Chief Information Security Officer will report serious computer security breaches to the Chief Information Officer (CIO) in a timely manner. The CIO will consult with one or more VP's as appropriate, and decide if the Critical Incident Management Team must be convened to determine a response strategy, or if an alternate group is appropriate for the response. This determination may be made prior to completion of the investigation of the security breach. The ISPO will report the incident to the Department of Public Safety, the appropriate Judicial Representative, and/or the University General Counsel when, based on preliminary investigation, criminal activity has taken place and/or when the incident originated from a University computer or network.

Determination of External Notification:

To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the (likelihood of the) following will be considered:

1. Physical possession (lost or stolen device?)
2. Credible evidence the information was copied/removed
3. Length of time between intrusion and detection
4. Purpose of the intrusion was acquisition of information
5. Credible evidence the information was in a useable format

6. Ability to reach the affected individuals
7. Applicable University policy, and/or local, state, or federal laws

External Notification:

If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

1. Written notice will be provided to the affected individuals using US Mail, unless the cost is excessive or insufficient contact information exists. The letter will be developed by the department responsible for the system experiencing the breach, and approved by University Relations and others as appropriate. The excessiveness of cost consideration will be the decision of the CIO, General Counsel, and Vice President for Finance and Operations.
2. If written notice to the affected individuals is not feasible, the following methods will be considered for providing notice:

- Personal e-mail notices (provided addresses are available), developed by the department responsible for the system experiencing the breach, and approved by the CIO, University Relations, and other administrators as appropriate.
- A press release to media, to be written by University Relations and approved by the CIO, and other administrators as appropriate.
- An informational web site, developed and hosted by the department responsible for the system experiencing the breach, and approved by the CIO, University Relations, and others as appropriate, with a conspicuous link in the University Home Page News area.

All expenses associated with external notification will be the responsibility of the department responsible for the system that experienced the security breach.

Definitions:

Private Information

If the information acquired includes a name (first and last name or first initial and last name) in

combination with any of the following, and the information was not in an encrypted format, a public notification may be warranted:

1. Social security number
2. Driver's license Number
3. Bank Account, Credit, or Debit Card Account number with security, access, PIN, or password that would permit access to the account
4. SSIUID Password

Personal information that is publicly and lawfully available to the general public, such as address, phone number, and email address are not considered private information for the purposes of this policy.

Highly Sensitive Information

If the information acquired is of a very sensitive, confidential, or proprietary nature, the security breach will be investigated and University officials, including the CIO, General Counsel, and Vice Presidents will determine if a public notification is warranted. Examples of highly sensitive information include but are not limited to:

1. Name, Address, with Date of Birth
2. Records protected by FERPA, HIPAA, GLBA, or other applicable federal laws and regulations
3. Research data or results prior to publication or filing of a patent application
4. Information subject to contractual confidentiality provisions
5. Security codes, combinations, or passwords

Related Policies, References and Practices:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Acceptable Use of Information Technology Resources Policy
Security Incident Escalation Policy
Institutional Data Access Policy

Guidelines for Classification of Institutional Data
Social Security Number Policy

Swarrnim Startup & Innovation University Gandhinagar

SWARRNIM STARTUP & INNOVATION UNIVERSITY
+91-95123 4333|info@swarrnim.edu.in|www.swarrnim.edu.in At Post Bhoyan Rathod, Near ONGC WSS,
Opp. IFCCO, Adalaj Kalol Highway, Gandhinagar, Gujarat- 382422

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT-24

Wireless-Networking-Policy

Description:

Provides guidance and procedures for the use of wireless technologies on the University of Iowa campus.This policy addresses the use of IEEE 802.11 wireless data networking protocols, commonly known as "Wi-Fi" or "wireless Ethernet." These protocols are used for connecting client devices to a data network through the use of over-the-air radio signals. The primary advantages of wireless networks are mobility and flexibility. The primary disadvantages are that wireless networks are more susceptible to service disruptions, and they operate at slower speeds.

Definitions:

1. IEEE 802.11 is a set of wireless networking protocols and standards adopted by the Institute of Electrical and Electronics Engineers (IEEE). The 802 committee works on data networking standards. The 802.11 subcommittee works on the subset of wireless standards that are commonly known as Wi-Fi. These standards define the components and functions of devices in an 802.11 network. These standards also include add-on definitions such as 802.11a, 802.11b, 802.11g, 802.11i, etc.
2. "Wi-Fi" is a term developed by the Wi-Fi Alliance to help identify devices that properly conform to the IEEE's 802.11 standards. The Wi-Fi Alliance was formed to help facilitate interoperability between wireless products from competing vendors.
3. Extended Service Set Identifier (ESSID or SSID) is the textual name of a wireless network. The SSID is used to identify the network and advertise its availability.
4. The phrase "wireless service" in this document refers to the University of Iowa wireless data networking service provided by Information Technology Services (ITS).

Policy Statements:

Swarrnim Startup & Innovation University ★ Gandhinagar

1. Access to the wireless service will be restricted to current students, faculty, staff, and guests that have been authorized.
2. Students, faculty, and staff shall be authenticated with their SSIU ID. Guests will be provided a Guest ID for authentication.
3. The wireless service shall protect authentication credentials through the use of data encryption.
4. Users of the wireless service are responsible for obtaining a device that meets the current implementation requirements.
5. The text "UI-Wireless" is reserved for defining SSID's for the University of Iowa wireless service. Wireless equipment in University owned or leased spaces that is not part of the University wireless service shall not include the text "UI-Wireless" in their SSID definitions.
6. ITS reserves the right to revoke wireless service authorization for an individual SSIU ID, Guest ID, or for any device that is disrupting the operation of the wireless service. Violation of the University of Iowa Network Citizenship policy or the Acceptable Use of Information Technology Resources policy will result in revocation of authorization to use the wireless service.
7. University faculty, staff, students and guests shall not install personal wireless networking equipment in University owned or leased spaces without written consent from ITS. See items 2 and 5 in the implementation section for more information, or contact ITS-NetworkServices@ssiu.ac.in.

Implementation of the Policy

1. Responsibility for implementing this policy rests with ITS. ITS is responsible for designing, configuring, installing, maintaining, and troubleshooting the University of Iowa wireless service.
2. ITS will maintain a written description of the current wireless data networking implementation in the form of a service description. This will include device requirements for accessing the network, and information regarding procedures to obtain authorization for the deployment of user supplied wireless equipment. This documentation will be available on the ITS Help Desk web site, at http://its.ssiu.ac.in/wireless
3. ITS will utilize central funding to provide a basic level of wireless service in libraries and many common areas. Wireless service expansion will typically be funded by the college, department, or unit requesting it.
4. ITS will provide a mechanism for procuring Guest ID's authorized to use the wireless service.

5. ITS is authorized to monitor/detect implementation of unauthorized wireless devices. ITS reserves the right to remove and/or disable wireless equipment that is in violation of this policy, and/or may disable any wired uplink data port associated with a device in violation of this policy.
6. For more information regarding the wireless service, send email to ITS-NetworkServices@ssiu.ac.in

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources).

1. Airspace Policy
2. Network Citizenship Policy
3. Acceptable Use of Information Technology Resources
4. Enterprise Login ID Standard
5. Enterprise Password Policy

Policy Number: IT-25

Network Address

Description:

This policy defines appropriate IP address use of global and other address ranges, with overall responsibility resting with Telecommunication & Network Services of ITS.The Telecommunication & Network Services (TNS) division of Information Technology Services (ITS) is responsible for planning, development, implementation and support of networking on the University main & Oakdale campuses. Coordination in the use of Internet Protocol (IP) addresses is included in this responsibility. The TNS Hostmaster (email hostmaster@ssiu.ac.in) is the service communication address for requesting IP address & hostname reservations. As

global, unique IP version 4 (IPv4) addresses are a finite and increasingly constrained resource, this policy defines appropriate IP address use of global and other address ranges.

Definitions::

Public IP addresses: Globally (or Internet) routable IP addresses are assigned by the Internet Address Numbering Authority (IANA). IP address ranges registered by the University of Iowa include:

128.255.0.0 – 128.255.255.255
129.255.0.0 – 129.255.255.255

Private IP addresses: IANA specifies IP address ranges for use exclusively within enterprise networks. Commonly referred to by the IEEE Internet Engineering Task Force document RFC1918, these are not routed to the global Internet. The IP address ranges specified in RFC1918 include:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Policy:

1. Systems requiring access to, or reachability from the global Internet should be configured with public (global) IPv4 addresses.
2. Individual or blocks of IP addresses not observed to be in use for a period of time, such as six months are subject to be reclaimed and reassigned by TNS with notice to the affected person, group, or place.
3. For use on University of Iowa networks, the 10.0.0.0 & 192.168.0.0 ranges of RFC1918 IP addresses are designated for use by system administrators on their local network without the coordination with TNS Hostmaster, or monitoring or enforcement by TNS.
4. The 172.16.0.0/12 range of private RFC1918 IP addresses are reserved for campus-wide or inter-campus applications such as the UI Anywhere VPN service and site-local scope routing of private IP addresses.
5. Campus system administrators may elect to implement host access-controls based on network address, but are responsible for conforming to the address ranges defined in the policy, and changes in address ranges that may occur in the future.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy. They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources).

Domain Name Policy
Network Citizenship Policy -

Policy Number: IT-26
Web Accessibility

The University of Iowa is committed to providing equal access to information, programs, and activities delivered through its official web resources. Official UI web resources include all web sites, web applications, and media delivered through the web used to conduct university business or academic activities. They include web resources purchased or delivered by outside vendors as well as those created on campus. They do not include personal resources published by students, employees or resources for non-university organizations that are hosted on campus but are not used to conduct university business or academic activities.
UI official web resources are to be designed and maintained in accordance with the standards defined in appendix A, UI Accessibility Standards and Resources. (The initial standard is the World Wide Web Consortium Web Content Accessibility Guidelines 2.0, Level AA.

See http://www.w3.org/standards/webdesign/accessibility.)

Implementation:

The effective date of this policy is November 1, 2011. After that date, all new web sites, new applications, or revisions to existing sites or applications are subject to this policy. Each unit managing web resources is expected to assess its current resources and make a plan for replacing or remediating existing web resources that don't meet accessibility standards. Existing resources should be updated according to the following schedule:

1) As required by accommodation requests. (University personnel should currently be considering modifications pursuant to accommodation requests.Please contact Student Disability Services or Faculty and Staff Disability Services for assistance in responding to such requests.)
2) At least the top 20% most active non-compliant resources should be replaced or remediated annually.
3) Special focus on web resources required for participation, funding, disability-related services, and other key pages needed by people with disabilities, if those pages are not among the top 20% most active.

Contact Information:

All University web resources must contain an accessible link a visitor with an accessibility concern can use to contact someone responsible for the resource. Resources should also include the date the resource was published and updated.

Exceptions to the Policy:

Exceptions to the policy are permitted only when full compliance would impose an "undue burden." In determining whether full compliance poses an undue burden, a department or unit must consider all resources available to it as well as the technical difficulty involved in complying with policy standards. A department or unit can depart from the policy only when it determines and documents to the ADA Compliance Officer that an undue burden exists that precludes full compliance; however, it must provide the content through comparable alternative means of access.

Complaints:

Address complaints to the ADA Compliance Officer in the Office of Equal Opportunity and Diversity.

Violations:

UI web resources in violation will be referred to the UI Web Accessibility Technical Standards Committee by the ADA Compliance Officer for assistance with remediation or replacement. Remediation may include removal until compliant with this policy.

Maintenance of policy:

This policy is maintained jointly by the offices of the Vice President for Strategic Communication and the Chief Information Officer. It is published on the IT Policy page, http://itsecurity.ssiu.ac.in/university-it-policy

Appendix A. UI Accessibility Standards and Resources Standards:

The current interim web standard is defined as compliance with the most current version of World Wide Web Consortium Web Content Accessibility Guidelines 2.0, level AA.
(See http://www.w3.org/WAI/intro/wcag.php)
This standard is subject to review and revision by the UI Web Accessibility Technical Standards Committee.
The UI Web Accessibility Technical Standards Committee is a standing committee chosen from senior webmasters at the college or major business unit level, application developers nominated by the Campus IT Leader in each college or major business unit, and others interested in web accessibility.
The UI Web Accessibility Technical Standards Committee plays the following roles:

- Advise on policy implementation
- Advise on technical priorities and goals of the web accessibility project
- Assist in measuring and monitoring progress of web accessibility project
- Identify needs of the wider web community for support and training
- Communicate policy and goals of the web accessibility project to constituent groups

Web accessibility resources will are published at the URL http://itaccessibility.ssiu.ac.in

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT - STANDARD 02

Enterprise Login ID Standard (SSIUID)

Description:

Provides the basis for a campus-wide standard for login IDs (SSIU ID) for all systems, including non-Windows operating systems.There is a widespread need for a login ID standard that can be applied throughout the enterprise. The initial enterprise login ID policy, adopted in April 2001, set the standard for IDs in thē campus Active Directory forest. Herein, this login ID standard is extended enterprise-wide to all systems, including Windows and non-Windows operating systems. Use of this standard login ID positions providers of campus IT services – central and locally managed – to utilize enterprise authentication. As campus IT providers adopt the SSIU ID standard, and the enterprise authentication service for the services they provide, the campus will benefit from the simplified sign-on environment.

Statement:

At the University of Iowa, the standard login ID is named the "SSIU ID." Local services may refer to this login ID by alternate names, but in all cases, the institutionally defined SSIU ID is the one reserved in the Enterprise Directory Service for each individual in the UI community.
SSIU IDs have these characteristics:

1. Because the initial assignment of SSIU IDs was based on existing IDs, there is diversity in the SSIU ID formats reflected in the UI community.
2. One SSIU ID is reserved for each person in the Enterprise Directory Service (EDS) at the time the person becomes known to the EDS.
3. SSIU IDs are between 3 and 30 characters in length. Any additional limits on length of a service login ID are determined by the requirements of each service needed by the end user. For example, there are services that can support only a maximum of 8 characters.
4. All uses of a specific SSIU ID must be associated with the same person that is assigned that SSIU ID in the EDS. That is, the login ID "jdoe" in service A must be assigned to the same person that the login ID "jdoe" is assigned to in service B.
5. The current default SSIU ID is a maximum 8-character alphanumeric string based on an individual's name.
6. Hyphens and underscore characters are, in general, used to denote service accounts and other exceptions to the SSIU ID standard. Therefore, punctuation, such as hyphens and

underscores, are not allowed in the SSIU ID, except in IDs based on hyphenated surnames.

7. There may be resource accounts (e.g., accounts for testing, departmental, generic use) in Active Directory for which there is no corresponding Enterprise Directory entry.
8. Creation and maintenance of SSIU IDs is an administrator responsibility. An end-user may request that his longer SSIU ID (greater than 8 characters) be changed or renamed to match his login ID on a system that limits login IDs to a maximum 8-characters.
9. A SSIU ID will be maintained for the life of services using it for authentication.

10.Whena login ID for service is required prior to completion of the institutional processes that result in assignment of a SSIU ID, a system administrator may reserve a SSIU ID for subsequent assignment to the person upon completion of the institutional processes.

11.As campus services adopt the SSIU ID standard, efforts to maintain existing login IDs will be balanced with active uses of the institutionally assigned SSIU ID.

12.The intent is that there will be a single SSIU ID (account) for each individual in the campus Active Directory forest. That is, a person's SSIU ID will appear in one and only one domain in the forest. This guarantees the uniqueness of the enterprise SSIU ID and SSIU ID password pair. Requests for exceptions to the single ID per individual rule may be based on role-based reasons. Exceptions must be approved by the appropriate domain administrators.

13.With the exception of temporary IDs provided by contractual services (e.g., applicants for professional colleges), there will be no individual user account established in the Active Directory for which there is not a validating, unique entry in the Enterprise Directory.

SSIU ID Changes It is expected that a SSIU ID will be changed only under a limited set of circumstances.

1. User and/or administrators may request a different SSIU ID for purposes of consolidation of services under another existing ID.
2. User and/or administrators may request a different SSIU ID in the event of a name change or if the auto-generated SSIU ID is inappropriate in some way.
3. Users and/or administrators may request a longer than 8 character SSIU ID so long as the current SSIU ID is not in use in a service and the requested SSIU ID is unique.

Campus service providers who adopt the SSIU ID standard may subscribe to the Enterprise Directory Change Log notification process.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources) by reference, per the Policy on Acceptable Use ofInformation Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

Enterprise Active Directory Policy
Enterprise Authentication Policy
Enterprise Password Policy
University ID Number Standard

Policy Number: IT - STANDARD 05

Computer Security Standard

Description:

A set of standards for the management of university owned desktop, mobile, and server computing devices, which are designed to minimize institutional risk.

Tens-of-thousands of computing devices are connected to the University of Iowa data network. These devices typically have access to institutional services and data. Automated, enterprise scoped system management is an effective method to reduce institutional risk with a reasonable

assurance of success. Threats to the privacy and integrity of institutional and personal information will continue to exist as long as there are financial, political, environmental, and/or criminal profits to be obtained. Automated computer management facilities can provide significant improvement in security, over manual computer management methods that are more time consuming and often less diligently applied to secure our assets. Scope: This standard applies to all university owned, networked devices such as desktop, mobile, and server computing devices. Some devices, such as clustered servers, firewalled or address obfuscated (NAT'd) servers, special purpose operating systems, or research devices may not be eligible due to licensing constraints, or may not support all management options, and therefore are expected to have comparable management implemented to the extent possible.

Statement:

1. **Domain Membership**: Register (join) all supported institutionally owned computing devices for directory-enabled management purposes. For example, devices with Windows operating systems, and Macintosh devices with OS X operating system, should be joined to the UIOWA (campus) forest via an authorized administrative "domain" unless granted an exception. Domain membership allows institutional best practice configuration policies to be automatically applied (via Group Policy Objects or GPO's) to many devices, enforces domain password policy, and also provides an inventory of assets.

2. **Automated System Management**: Subscribe all supported institutionally owned computing devices to an authorized management environment (e.g., Central SCCM or Casper service) for automated updates of both operating system and application software. Utilization of automated management solutions for client security (i.e., anti-virus, anti-spyware, intrusion prevention, or data loss prevention) is also required for eligible (supported) devices.

3. **Update/Configuration Parameters**: Institutionally owned computer systems, in addition to the baseline requirements outlined in the University's Network Citizenship Policy, should be configured to utilize automated system management to:

- Configure and apply updates to the operating system at least monthly, with reboot as necessary
- Apply updates to installed software, including plug-ins, at least monthly
- Only install/utilize supported versions of software from companies or sources (for open source software) that actively provide updates
- Implement a managed version of client security software where possible, that updates at least daily, and actively scans all incoming files

4. **Confidential Data Physical Protection**: Protection of confidential data must adhere to the Institutional Data Access Policy.

5. **Duplicate Services**: Limit the number of services that must be protected, by avoiding development and implementation of parallel (duplicate) IT systems. Examples include Active Directory Forests/Domains, E-mail servers, and Servers hosting SQL and Oracle databases. This is not intended to eliminate redundancy or backups for disaster recovery or survivability of important resources, but rather to reduce the potential points of attack and avoid costs to secure and monitor duplicate systems.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy. They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

Information Security Framework Policy
Network Citizenship Policy (includes Baseline Security Standards)
Institutional Data Access Policy
Self-managed machine responsibility/checklist
Ulowa System Registry (USR) application

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE

INDIA'S FIRST UNIVERSITY FOR STARTUP

Swarrnim Startup & Innovation University
Bhoyan Rathod, Gandhinagar

Swarrnim Startup & Innovation University
Gandhinagar

SWARRNIM STARTUP & INNOVATION UNIVERSITY
+91-95123 4333|info@swarrnim.edu.in|www.swarrnim.edu.in At Post Bhoyan Rathod, Near ONGC WSS,
Opp. IFCCO, Adalaj Kalol Highway, Gandhinagar, Gujarat- 382422

SWARRNIM
STARTUP & INNOVATION
UNIVERSITY
WHERE IDEAS COME ALIVE
INDIA'S FIRST UNIVERSITY FOR STARTUP

Policy Number: IT - STANDARD 22

Computer Security Standard

Description:

Provides a standard identification number for students, faculty, staff and affiliates when they have established a recurring business relationship with the University of Iowa.The University ID Number (Univ ID) was implemented to provide a standard identification number for students, faculty, staff and affiliates who have an established business relationship with the University of Iowa. The Univ ID is intended to replace Social Security Number (SSN) as an individual's principle identifier within the administrative and academic information systems utilized on campus. SSN will be retained as an attribute of a person, similar to date-of-birth and residing address, as outlined in the "Social Security Number Policy." This standard describes a method of unique identification designed to protect the privacy of individuals, while allowing them to easily identify themselves when transacting business with the University of Iowa.

Policy:

1. Univ ID is an immutable 8-digit, identification number which is unrelated to any SSN. It provides a one-to-one unique link in the institutional directory service to other attributes of one's relationship with the University.
2. Univ ID numbers are pseudo-public identification numbers which are used by all services and administrative and academic information systems developed and acquired by the University. Univ ID will be printed on the UI ID Card, unless the card holder requests that it be omitted.
3. Univ ID numbers, or other tracking numbers such as invoice numbers, will be used in lieu of SSN in all electronic and paper data systems to identify, track and service individuals with a recurring business relationship with the University.
4. Compliance will require our best efforts to change procedures, systems, reports and other printed materials that do not require the SSN as essential information within such system, transaction or report. Therefore, it does not define a specific timeframe for compliance, but periodic assessments of compliance may be made, as appropriate.
5. Univ ID is considered property of the University and its use and governance shall be at the discretion of the University, within the parameters of the law.
6. Univ ID numbers will be maintained and administered by Information Technology Services (ITS).

7. Grades and other student-related pieces of personal information will not be publicly posted or publicly displayed in a manner where either the Univ ID or SSN, or any portion thereof, identifies the individual associated with the information.

Related Policies, References and Attachments:

This collection of University of Iowa Information Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Iowa policy.
They are incorporated into the University of Operations Manual (http://opsmanual.ssiu.ac.in) by reference, per the Policy on Acceptable Use of Information Technology Resources (http://opsmanual.ssiu.ac.in/community-policies/acceptable-use-information-technology-resources)

University Social Security Number Policy
Acceptable Use of Information Technology Resources
Institutional Data Access Policy

Attachments:

1. Accepted entry points for creation of Univ ID (current 8/2006):
2. Admissions
3. Registrar (SRIS)
4. Guided Independent Study Student System
5. Human Resources
6. University ID Card Services (when required for card creation)
7. UIHC Staff Relations (when required for badge creation)
8. Enterprise Directory Service (when IT services required)
9. University Libraries (planned)

- Campus Applications Implementation Guidelines (to be written).

Swarrnim Startup & Innovation University
At. Boyan Rathod, Gandhinagar.

Swarrnim Startup & Innovation University ★ Gandhinagar