Ibn Sina University
Information & Communications Technology (ICT) Security Policy

Contents

PURPOSE

The purpose of this policy is to protect Ibn Sina University's Information and Communications Technology (ICT) resources from accidental or malicious disclosure, modification, or destruction, while also preserving the open information sharing requirements of its academic culture.
This policy lays the foundation for a common understanding of information security at ISU based on the generally accepted information security principles of confidentiality, integrity and availability, in particular "International Standard ISO/IEC 27002:2005. Information technology - Security techniques - Code of practice for information security management".
Confidentiality limits information access to authorised users.
Integrity protects information against unauthorised modification.
Availability ensures that information is accessible when needed.
The Officers of the University expect University information in any form, and related assets, to be accurate, available for authorised use, and protected from misuse or modification.
Information security management enables information to be shared while ensuring protection of that information and its associated computer assets. Ibn Sina University's Executive Management Group is responsible for ensuring appropriate controls are in place to preserve the security objectives of confidentiality, integrity and availability of Ibn Sina University's information assets.
Information that ISU or its agents use in the course of conducting University business is an institutional resource. Although individuals, departments and schools may have responsibility for creating and maintaining portions of University information and University records, the University itself retains ownership of, and responsibility for, the information.
This document describes the overall high-level ICT Security Policy for ISU. It is complemented by a series of sub-policies each of which defines more specific security policies for individual components of the ICT environment (e.g. Updating, Network Connectivity, Remote Access etc). These sub-policies and related documentations are published and accessible on the ISU website.

SCOPE

This policy applies to faculty, staff, students, and all others granted use of University information or related assets and defines their responsibility for the protection and appropriate use of University information, applications, computer systems and networks. It applies to all ICT domains within ISU and includes those domains managed centrally.

as well as those managed within Schools/Units. The policy applies to associated colleges to the extent that they use ISU's ICT assets.
Within the context of this policy, information refers to all information processed, stored, used or transmitted in any medium or form. Information resources include, but are not limited to: ISU's network, computers, workstations, software, hardware, Internet, e-mail, handheld devices, voice mail, cellular phones etc. The scope includes the physical protection of the ICT assets.

ICT SECURITY POLICY

Custodianship and Protection

All assets associated with information systems including information assets, software assets, physical assets, and services have a defined asset custodian. The custodian has overall responsibility for the integrity, availability and protection of the asset.
ISU retains overall responsibility and ownership for all University records, information and ICT assets.
Individuals, Schools and Units etc are tasked, as custodians, with creating and maintaining these assets.
Custodians of ICT assets are responsible for the protection, integrity and availability of those assets and for putting the appropriate controls and procedures in place. Tangible assets are to be located in appropriately secure physical locations.
Examples would include: ISS are custodians of Internet Access Infrastructure, Registry are custodians of Student Data, Finance are custodians of Finance systems etc.

Confidentiality and Privacy

The University and all members of the University community are obligated to respect the rights of individuals and to protect confidential data.
Attention is drawn in particular to the:
Code of Conduct for the Use of Computing Resources at ISU
Breaches of the Code of Conduct for the Use of Computing Resources in ISU and
Guidelines on Data Protection Acts 1988 and 2003

Integrity

Custodians of ICT assets are responsible for the integrity and accuracy of those assets.

Controls and processes need to be put in place to ensure assets are accurate, up-to-date and protected from unauthorised modification.
Regular monitoring must be carried out to ensure effectiveness.

Availability and Access

Custodians of ICT assets have responsibility to ensure that the assets are available when needed and that access to those assets is restricted to authorised entities only.
No one may access records unless specifically authorised to do so. Authorised individuals may use records only for authorised purposes.
Custodians must satisfy themselves that appropriate arrangements and procedures are in place to ensure ICT assets, for which they have responsibility, are available for access when required.
Custodians will also ensure that controls are in place to avoid unauthorised intrusion of systems and networks and to detect efforts at such intrusion. Such controls could include: Password rules and management, traffic monitoring, analysis of intrusion attempts, port scanning etc.
Custodians of assets will also ensure that administrative access procedures include provisions for alternative administrative access in the event that the primary access holder is incapacitated or otherwise unable to perform the required administrative activities.

ICT Incident Response

An **ICT Security Incident ("Incident")** is defined as any activity that harms or represents a serious threat to the whole or part of ISU's computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems. This includes unauthorised access or changes to, or theft of hardware, firmware, software or data, or a crime or natural disaster that destroys access to or control of these resources. It also includes the use of ICT resources in a manner that constitutes a criminal act. Information on the routine detection and remediation of a "virus," "malware" or similar issue that has little impact on the day-to-day business of the University can be found at: http://www.ISU.EDU.SD/iss/security-anti-virus.shtml
 All ICT Security Incidents must be reported without delay to the local ICT administrator where appropriate, to the Head of School or Unit and to the Information Systems and Services (ISS) Department.

 Evidence relating to a suspected Information Security breach should be recorded and, where necessary, disclosed to the Director of ISS.

 All employees should be made aware that evidence of information security incidents may be formally recorded and retained.

 Users of information systems are required to note and report any observed or suspected security weaknesses in, or threats to, systems and services. Such weaknesses or threats should be treated as security incidents, and be reported promptly.

 Wherever possible, the University will undertake to prevent incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its ICT resources.

- Security Incidents reported to ISS will be subject to appropriate internal procedures. These procedures will be reviewed periodically to adjust processes, identify new risks and remediation.

Responsibilities

ISU Executive

 The ISU Executive Group has overall responsibility for the University's ICT Security Policy to protect the assets of the University.

 Appropriate policies must be in place together with management, monitoring and review procedures to ensure policies are implemented, adhered to and kept up-to-date.

ICT Security Implementation Group

 Oversee the ICT Security Agenda for ISU – make recommendations to Executive and report on ICT Security matters.

 Prioritise the recommendations outlined in the Security Review.

 Oversee the implementation of ICT Security Policies and Procedures and report on progress.

Custodians of ICT Assets

 The Custodians of ICT assets have key responsibilities within the context of the ICT Security Policy.

 The high level responsibilities are described in the sections above addressing: Custodianship & Protection, Confidentiality & Privacy, Integrity and Availability & Access.

 Ensure that all ICT assets being acquired/introduced adhere to University Policies and Procedures.

Computer Users

 Individual users are responsible for ensuring that others do not use their system privileges. Users must:

 Protect their username and password from inadvertent disclosure

 Passwords should never be loaned to others

 Individual users will be held responsible for any security violations associated with their usernames

 Ensure that all ICT assets being acquired/introduced adhere to University Policies and Procedures.

 Be aware of their responsibilities under Staff Policies & Procedures and ensure compliance with them.

Information Systems & Services

 Play a key role as one of the main stakeholders on the ICT Security Implementation Group

 Implementation of Security Policies for centrally managed facilities for which it has custodianship.

 Review incident logs and identify potential security violations.

 Provide advice and assistance to support the implementation and management of ICT Security Policies and Procedures.

Note: A similar role to that of ISS staff members is played by System Aministration staff within Schools and Units.

Third Parties

In the normal course of events, ISU's Information Systems & Services,and other Schools or Units may contract for services. Representatives of these contracted companies must follow all University policies.

Schools and Units are expected to establish appropriate guidelines for building, equipment and system access. It is the responsibility of the contracting School/Unit to inform the contractor of all appropriate policies and, in addition, to provide oversight of the contractor and contractor representatives during the time they have access to University resources.

COMPLIANCE and EXCEPTIONS

 Compliance with this policy is mandatory. Each user must understand his/her role and responsibilities regarding information security issues, and protecting Ibn Sina University's information assets. Any non-compliance with this or any other security policy that results in the compromise of ISU information confidentiality, integrity and/or availability may result in disciplinary action and possible prosecution under applicable legislation.

 Any compromise or suspected compromise of this policy must be reported as specified in: Breaches of the Code of Conduct for the Use of Computing Resources in ISU

 Exceptions to the Information Security policy will only be granted if an appropriate business justification for the exception is approved and the person requesting the exception fully accepts the additional risk posed by the exception.

 A business justification describing the reason for the exception must be documented in writing, and submitted for approval by the ICT Security Implementation Group to the Director of the Information Systems & Services.

DEFINITIONS

ICT Assets

Applications, computer systems, servers, networks and related devices owned by or entrusted to the University.
Examples of ICT assets are:
Information assets: databases and data files, customer information, developed industry information, competitive information, research and development technical information, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information;
Software assets: application software, system software, development tools and utilities;
Physical assets: computer equipment (e.g. processors, monitors, laptops, modems), communications equipment (e.g. routers, PBXs, fax machines, telephones), magnetic media (e.g. tapes and disks), other technical equipment (e.g. power supplies, air-conditioning units), furniture, and accommodation;
Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

University Information

All information that the University or its agents use in the course of conducting University business.

Continuity of Operations

Continuity of Operations plans and arrangements ensure that there are mechanisms in place to maintain, or quickly resume, essential services and operations within the University in the event of a catastrophic event (e.g. fire, flooding etc) that results in disruption of normal activities and services within the University.

DOCUMENT INFORMATION

Ibn Sina University believes that it is important to keep this Information Security Policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed.
The Director of Information Systems & Services will draft necessary changes and have them reviewed and approved by the Executive Group of ISU as appropriate. The Director of ISS and the members of the ICT Security Implementation Group will communicate changes to the University communities. Anyone in the university can determine the need for a modification to the existing policy. Recommendations for changes to this policy should be communicated to the Director of ISS.