KING FAISAL UNIVERSITY

Information Security Policy

version 2.0

Prepared & Presented by:

M. Shahul Hameed,
MBA, M.Sc.IT, C\MA, CIA, PMP, CGEIT, CISA, CISM, ITSM(ITIL), ISO27001LA,

Head of Quality Management Office, Deanship of IT

Arabic Translated by:

Ahmed Samir Morsy,
BEng, PGSD CS, MCTS, MCT, MCSD, MCAD, MOS

Assistant to Head of Quality Management Office, Deanship of IT

http://kfu.edu.sa

Table of Contents

1- Introduction (1/2)

With the increasing speed of new technology strategies and stakeholders expectations, protection of information assets has become paramount, and subject to have continuous improvement in light of industry standard best practices concerning information security.

This framework and policy, including the sub policies, procedures and guidelines apply to all KFU community that includes employees, contractors, consultants, temporaries, faculty, students and all others who have been given access to the KFU information systems as well as all other access to any third party information systems that are connected through KFU network.

1- Introduction (2/2)

- The **owner and responsible** party for the management of this policy is the **Dean of Information Technology**.
- **Information Security Manager** (ISM) will be the **primary contact point** on the implementation and maintenance efforts of the KFU.
- Head of Quality Management Office of the Deanship of IT will assume the role of the ISM, until a specific assignment is made by the dean and the **Quality Management Office shall be the coordinator in establishing this policy** as well as supporting the monitoring and control of its effectiveness for meeting the business requirements.

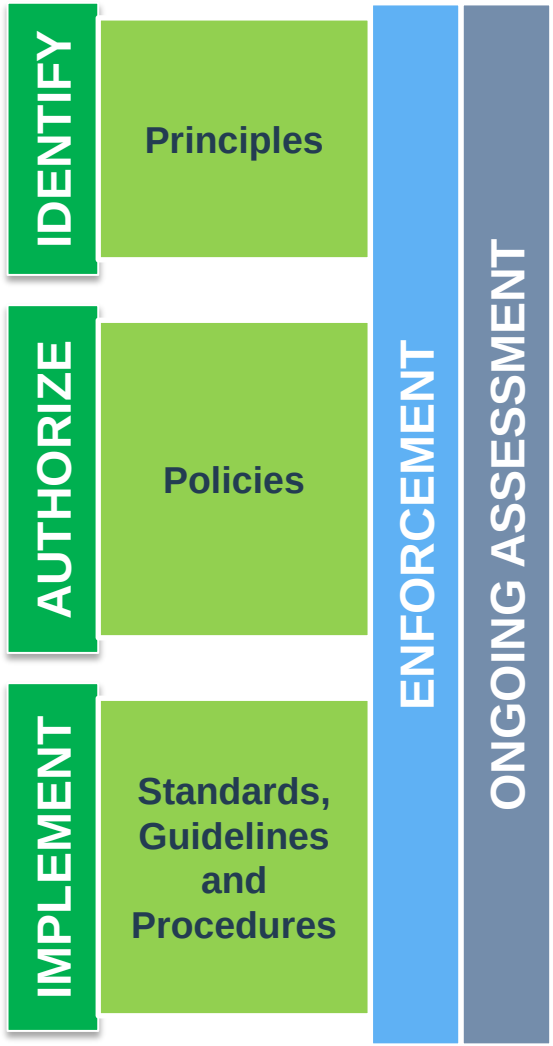
Table of Contents

2- Information Security Framework (1/2)

This **policy manual has been prepared in light of best practices,** which are considered as prudent control measures for safety and security of information and related technology.

- Policy Framework
- Information Security Governance
- Information Security Baseline
- Information Security Governance Committee
- Information Security Governance Committee Meetings & Proceedings
- Information Security Governance Committee Members
- Information Security Management Processes (ISMS)
- Deliverables of the Information Security Management Process

2- Information Security Framework (2/2)



Identify:
- Principles and Policies
- Standards
- Guidelines and Procedures

Authorize:
- Enforcement
- Controlled Environment

Implement:
- Authorized courses of action
- Security Controls
- Awareness Programs

Enforcement:
- Technical controls
- Penalty clauses
- Security incident reporting
- Follow-up

Ongoing Assessment:
- Respond to change due to business models change, new technologies
- Respond to change due to regulatory compliance requirements
- Respond to change due to availability of improved control measures against increasing risks, based on cost-benefit analysis and business demands.

Table of Contents

3- Information Assets – Identification and Classification

Information Assets Database

- All definable piece of information, stored in any manner which is recognized as “valuable” to the organization is to be considered as information assets.
- A project plan to be prepared for building or improving / enhancing any existing tool for the configuration management of all information assets.
  - In the absence of a sophisticated information management tool for CMDB (Configuration Management Data Base), during the interim period, any office automation tool such as excel or access database could be used in order to collect the information assets list as updated with all classification parameters.

Information Classification and Protection Requirement

- General (“PUBLIC”)
- Proprietary (“FOR INTERNAL USE”)
- Restricted (“PRIVATE”)
- Secret (“CONFIDENTIAL”)

Table of Contents

4- Risk Assessment

- **Risk assessment** process assess potential business impact, evaluating threats and vulnerabilities and selecting appropriate controls **to meet the business requirement for information security** in a system in a cost effective manner.

- **Quality Management Office** of the Deanship of IT (QMO) has been assigned with responsibility **for leading the coordination** with Operational Risk Specialists and Auditors in all such activities **relating to risk assessment and risk management process**.

- **All departments and deanships should identify a coordinator** for their organization and ensure all communications between their organization and Quality Management Office of the DIT.

Table of Contents

5- Information Security Policy (1/3)

Information Security Objectives

- To **ensure awareness** of information security to all users at least annually once or within two months of their joining the KFU.
- To **perform Risk Assessment and Business Impact Analysis** for all critical information assets at least once in two years and also prior to each major changes to any critical information assets.
- To **publish periodical report to the Information Security Governance** Committee with regard to the status of information security of the KFU.
- To **ensure updating of centralized inventory of all IT assets across the KFU** before being issued or implemented.
- To **ensure implementation of cost-effective controls in order to protect the information assets** and provide effective and efficient monitoring and control procedures for evaluating the implementation **and maintenance of information security policy across the KFU.**

5- Information Security Policy (2/3)

Approval of Policies and procedures

- All policies on Information Security **should be approved by the President** or Vice President for Studies, Development, and Community Services, based on the recommendations of the Dean of Information Technology and the Information Security Governance committee resolution.

- **All procedures and guidelines, including sub policies** relating to the approved policies established for the purpose of implementing and maintaining the main information security framework and policies **shall be approved by the Dean of Information Technology**, based on the recommendation by ISM.

Revision of Policies and Procedures

- This policy will be fully **reviewed at least once in 2 years** in order to reflect the new risks and changes to the business environment.

- It will be **amended** between full reviews if regulatory, control, or organizational development warrants a **change** in the policy.

- **Suggestions** for improving the content of this policy should be addressed to shahul@kfu.edu.sa (Head of QMO of the Deanship of IT).

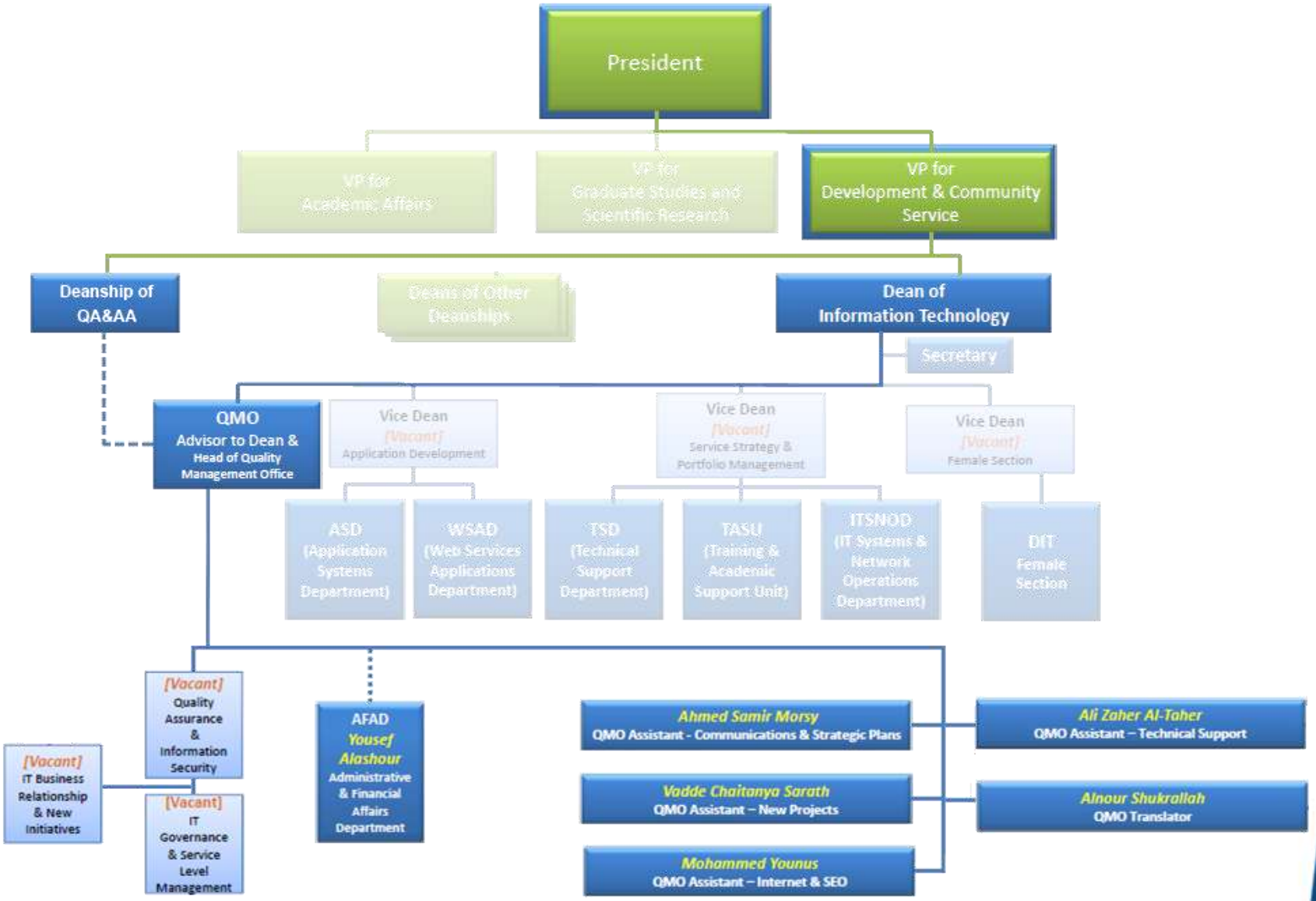
5- Information Security Policy (3/3)

List of Policies, Procedures, Guidelines and Checklists

- The Quality Management Office of the Deanship of IT, will maintain the list of all the current and relevant policies, including sub policies, procedure and guidelines prepared by all IT departments and publish them in the DIT website.

Table of Contents

6- Organization of Information Security Management (1/2)



6- Organization of Information Security Management (2/2)

- Internal Organization Policy
- Management Commitment
- Information Security Coordinators
- Information Security Roles and Responsibilities
- Authorization process for Information processing facilities
- Confidentiality Agreements
- Contact with Authorities
- Contact with special interest groups
- Independent Review of Information Security
- External Parties Policy (www.mohe.gov.sa and other regulatory policies)

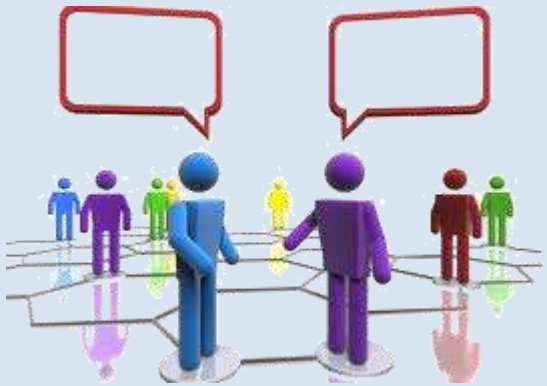


Table of Contents

7- Asset Management Policy

- Responsibility for Assets – Inventory Control.
- Responsibility for Assets - Ownership of Assets.
- Responsibility for Assets – Acceptable Use of Information Systems.

Table of Contents

8- Human Resources Security Policy

Prior to employment

- Roles and Responsibilities.
- Screening.
- Terms and conditions of employment.

During Employment

- Management Responsibilities.
- Information Security Awareness Education and Training.
- Disciplinary process against a security breach.

Termination or change of employment

- Hand-Over Procedures

Table of Contents

9- Physical and Environmental Security Policy

- KFU has a Department of Security and Safety under its Administrations group of the organization structure.
- All policies and procedures for the KFU's security perimeter are governed by this department's policies, procedures, guidelines and circulars.

Table of Contents

10- Communication & Operations Management Policy (1/5)

Operational procedures and responsibilities

- Documented Operating Procedures.
- Change Management.
- Segregation of Duties.
- Separate Development, Test and Production facilities.

Third-party Service Level Management

- Standard SLA's – Service Level Agreement
- Security Controls, Service Definitions, Delivery Levels
- Checklists for ensuring controls

10- Communication & Operations Management Policy (2/5)

System planning and acceptance

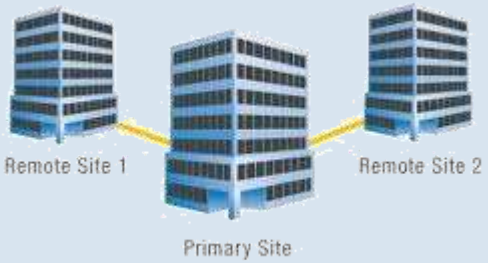
- Capacity Management.
- System Acceptance Criteria for development and testing.

Protection against Malicious and Mobile code policy

- Detection, prevention, and recovery controls to protect against malicious code .
- Appropriate user awareness procedures.
- Authorized mobile code definition

10- Communication & Operations Management Policy (3/5)

Backup and Recovery Policy



- Application system reference
- Data scope (folder) reference
- Backup/restore script/procedure identification
- Frequency of the backup and Recovery Point Objective (SOD/EOD etc.)
- Retention period
- Off-site location and tape library id etc.

Network Security Management Policy

- General issues related to Communications and Network Security
- Network Security Architecture
- Network Infrastructure Management
- Network Infrastructure Monitoring
- Communications and Network Security Audit

10- Communication & Operations Management Policy (4/5)

Media Handling Policy

- Handling of physical media
- Authorize to individual personnel
- Appropriate risk migration measures

Policy for Information Exchange

- Information Exchange.
- Exchange Agreements.
- Transportation of Media.
- Electronic Messaging.
- Interfaces and interconnection of business information systems.

10- Communication & Operations Management Policy (5/5)

Electronic Commerce services policy

- Electronic Commerce
- On-line transactions
- Public available information

Monitoring Use of Information Processing Facilities Policy

- Audit logging
- Monitoring system use
- Protection of log information
- Administrator and Operator logs
- Fault logging
- Clock synchronization

Table of Contents

11- Access Control Policy (1/2)

KFU requirements for access control

- Access control policy.

User Access Management

- User registration.
- Privilege Management .
- Password Management .
- Periodical Review of User Access Rights.

User Responsibilities toward access control policy

- Users must follow good security practices
- Users must ensure that unattended equipment has appropriate protection

Users must be updated with Acceptable Use policy

Network Access Control

- Information Access restriction.
- Sensitive system isolation.

11- Access Control Policy (2/2)

Operating system access control

- Operating System security parameters
- Assessment of compensating controls
- User identifier and user authentication mechanism
- Single sign-on

Application and information access control

- Information Access Restriction.
- Sensitive System Isolation.

Mobile computing and Tele-working

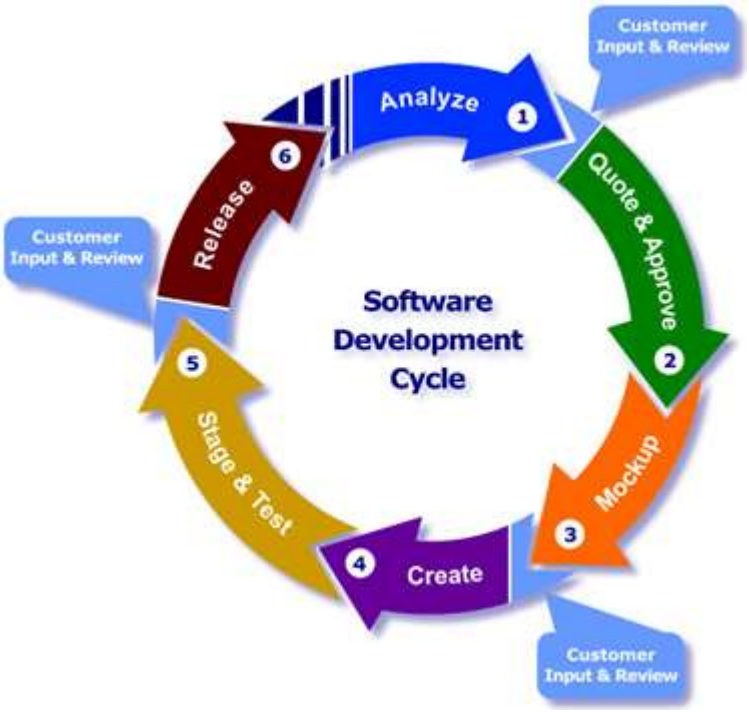
- Mobile computing and communications.
- Tele-working (off-site computer usage).

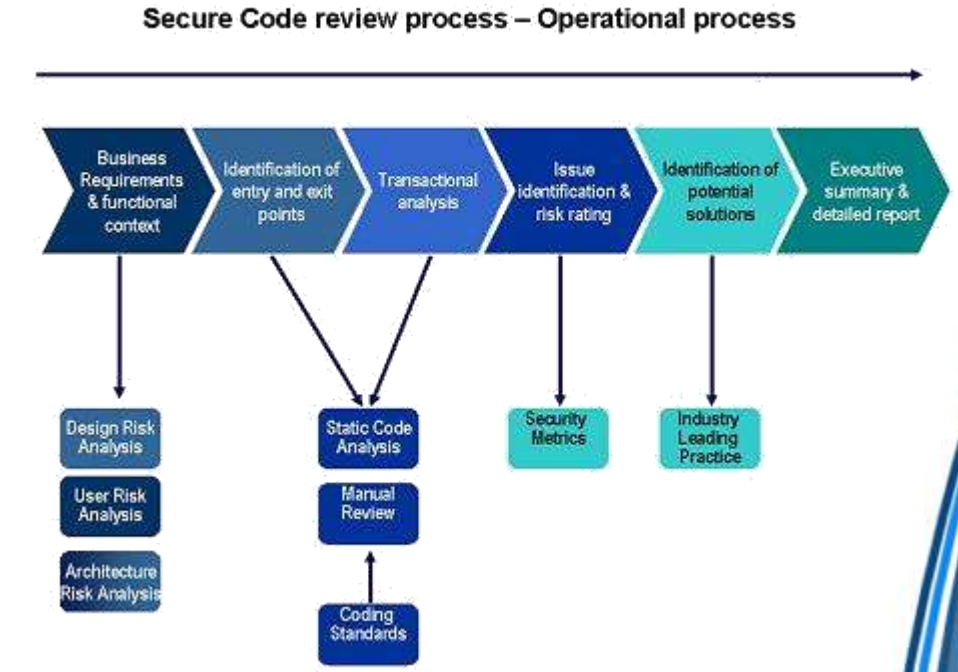
Table of Contents

12- Security Controls on Systems Acquisition, Development & Maintenance (1/3)

System Development and Life Cycle Methodology

- Security Requirements of Information Systems.
- System Development Life Cycle (SDLC) methodology.





12- Security Controls on Systems Acquisition, Development & Maintenance (2/3)

Correct Processing in Applications

- Data input validations – Automated or integrated
- Verification of input sources
- Authenticity and protecting message integrity

Cryptography and Key Management

- Cryptographic Controls Policy.
- Key Management.

Security of System Files

- Operational Software.
- Protection of System Test Data.
- Access Control to Program Source Code.

12- Security Controls on Systems Acquisition, Development & Maintenance (3/3)

Security in development and support processes

- Change control procedures.
- Technical Review of Applications after operating system changes.
- Restrictions on changes to software packages.
- Information leakage.
- Outsourced software development.
- Technical Vulnerability Management.

Table of Contents

13- Information Security Incident Management Policy

- Reporting information security events, Security events relating to operational risk should be reported to Information Security Governance Committee through the QMO of DIT.
- Reporting security weaknesses.
- Management responsibilities for ensuring quick, effective, and orderly response to information security incidents.

- Effective and efficient mechanism for learning from information security incidents.
- Collection of evidence in support of legal proceedings.
- Creation of appropriate awareness among all users periodically.

Table of Contents

14- Business Continuity Management (BCM) Policy

The information security aspects of business continuity management should be governed by a set of policies, procedures, guidelines and checklists and the same should include the following controls

- Developing & maintaining a managed process.
- Each deanship and departments of the KFU should ensure that BCM exists for them.
- All events that can cause interruptions to business processes should be identified, Business impact of these threats should be analyzed in consultation with the process owners and the asset owners/custodians in prioritizing for recovery and preparing the business continuity and recovery plans.
- Developing & implementing detailed plans and procedures.
- Maintaining a single framework of business continuity plans to ensure all plans are consistent.
- A designated person shall be nominated as the BCC (Business Continuity Coordinator, who is the owner of BC Plan and processes) for each critical deanship and/or departments.

Table of Contents

15- Compliance Policy

- Compliance with Legal Requirements.
- Compliance with security policies and standards, and technical compliance.
- Information systems audit considerations.

وزارة التعليم العالي
MINISTRY OF HIGHER EDUCATION

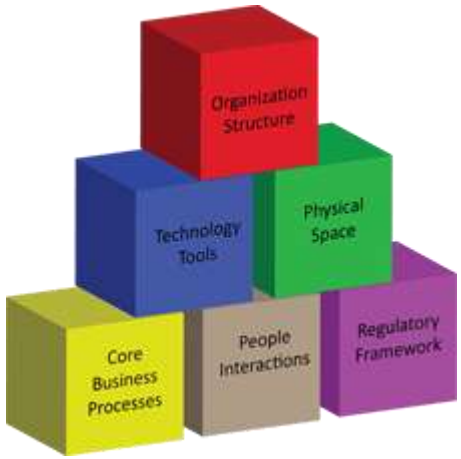


Table of Contents

16- Disciplinary Action and KFU Rights

- Users responsibility for compliance with regulatory and KFU information security policy obligations.
- Protecting Evidence from Destruction.
- Disciplinary Action and Legal Issues.
  - Intellectual Property Rights
  - Deactivation of User Accounts / User Names
  - Internet and E-mail Access Revocation
  - Collection of Usage Statistics
  - Communications Monitoring
  - Enforcement

Thank You

شكراً لكم

KING FAISAL UNIVERSITY

Deanship of Information Technology

جامعة الملك فيصل

عمادة تقنية المعلومات

Please contact: **M. Shahul Hameed** [shahul@kfu.edu.sa] for information

لمزيد من المعلومات يرجى الاتصال بـ: **محمد شاهول حميد** - البريد الالكتروني: shahul@kfu.edu.sa