KINGDOM OF SAUDI ARABIA
Ministry of Higher Education
KING FAISAL UNIVERSITY

المملكة العربية السعودية
وزارة التعليم العالي
جامعة الملك فيصل

# Information Security Framework and Policy of King Faisal University

[Framework and Policy Manual]

Owner: KFU-DIT-QMO

**Quality Management Office, Deanship of Information Technology**

Version 1.0 May 2011

## Document Control Information

| Document Details | |
|---|---|
| Document Name | KFU-DIT-ISP-Information Security Framework and Policy Manual |
| Purpose of Document | Establishing Information Security Framework for the King Faisal University. Provide a baseline for detailed implementation of security controls as per best practices. |
| Document Version Number | 2011 v1.0 (Initial) |
| Document Status | Live |
| Document Owner | Dean of Information Technology |
| Prepared By | M. Shahul Hameed, MBA, M.Sc., CMA, CIA, PMP, CISA, ITIL Advisor to Dean & Head of Quality Management Office, Deanship of Information Technology |
| Date of First Draft | May 2011 |
| Date Approved | Sent for peer review and approval during Oct 2011 |
| Approved By | Dean of IT & VP For Development and Community Services (email dated 24-11-2011) |
| **Next Scheduled Review Date** | May 2013 |
| **Classification** | Public (portion relating to “INTERNAL USE” are specifically mentioned and removed from the publication. |
| **Number of Pages / File Size** | 68 pages (excluding annexure) |

## Document Change History & Version Control

| Function | Name | Title | Version | Signed Date |
|---|---|---|---|---|
| Prepared by (Initial draft proposal) | M. Shahul Hameed | Advisor to Dean & Head of Quality Management Office, Deanship of IT | V 1.0 | 10-Oct-2011 |
| Assisted by (ARABIC translation) | | Professional Translators working under DIT/QMO | V 1.0 | |
| Review by | Peers | Deanship of Quality Assurance & Academic Accreditation | V 1.0 | 23-11-2011 |
| Validated & Approved by | Dr. Mohammed S. Al-Zahrani | Dean of Information Technology | V 1.0 | 24-11-2011 |
| Approved by | Dr. Ahmed A. Al-Shoaibi | Vice President For Development & Community Service | V 1.0 | 24-11-2011 |

## Distribution list:

| No. | Name/Group | Title | Department/Deanship |
|---|---|---|---|
| 1. | All Staff, including third party personnel, other than managers and system/security administrators need to be distributed with the general set of policies that are applicable for all persons for the purpose of enforcement of this policy.<br><br>Further detailed and for " INTERNAL USE " policy and procedures shall be made available through the intranet as well as email publications to all applicable uses and department heads, through whom the same shall be distributed to all parties involved. | NA | All Departments and Deanships |
| 2 | All system administrators (the complete set of policy manual other than critical part relevant only for the security administrators and the business owners or department/section managers.) | IT staff | Deanship of IT and Deanship of eLearning |
| 3. | All security administrators (the complete set of policy manual excluding any critical area of concern that is not relating to his job area but including all relevant portions for technical implementation and maintenance of policy should be covered) | IT staff | IT Security Team under Quality Management Office of the Deanship of Information Technology. |
| 4. | All policy review and approving authorities (complete set) | N/A | KFU Senior Management, Deanships of IT, and QAAA. |

# Table of Contents

# 1. Introduction

## *1.1 Background*

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.

Though there was no compiled information security policy manual as such, the King Faisal University (KFU) information security management procedures were effective, to certain extent, as it was considered as achieved by way of establishing interim policies, procedure memos and circulars; and also implementing critical information security related automated controls in order to maintain the security requirements of the university on timely basis.

Now, as part of the major initiatives undertaken in the Strategic Plan for 2011 to 2015, it is time to completely review and restructure the same with updated information and rules in light of available efficient and effective controls in order to implement immediately as the management tool to mitigate the increasing risks cost-effectively.

As initiated by senior management of the university and the deanships, and also acknowledging with thanks to the regulatory requirements of the ministry of higher education as well as the academic accreditation standards, we have arrived at formulating this framework and policy manual aimed to deliver a robust baseline tool for the purpose of immediate implementation across the KFU and its community areas of concern.

Therefore, the appropriately extracted and interpreted portions of this new policy manual, referred as KFU-DIT-ISP Information Security Framework and Policy 2011 v1.0, shall be published through the www.kfu.edu.sa website so that it should come into enforcement with immediate effect as on the date of the approval of this policy.

## *1.2 Objective*

The objectives are to:

- Select and include an appropriate framework for setting control objectives and establish an overall sense of direction and principles for action with regard to information security.
- Take into account business and legal or regulatory requirements, and contractual security obligations.

- Align with the university's, ministry of higher education (MOHE)'s, and its affiliated members risk management context in which the establishment and maintenance of the Information Security Management will take place.
- Ensure risk evaluation per criteria as set by Risk Governance of the senior management of the university and and implement cost-effective preventive, detective and corrective control measures as per approval by competent authorities.

### *1.3 Scope*

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.

However, the responsibility of KFU with regard to all third party information technology domains that has been connected with KFU's primary and/or other critical network, must be covered by a specifically written service level agreement (SLA) or any other contract, signed by both parties, which should clearly specify the scope of information security management by KFU's information security responsibility.

It is to be noted that where ever the term 'organization' or 'university' or 'KFU' is mentioned for denoting the scope coverage of a policy or procedure, then it is referring to the King Faisal University and its coverage area of providing the service to its community.

Wherever this policy refers to 'employee' or 'user' it should be understood that it actually refers to all authorised KFU community members depending on the case or situation that the policy is actually referring. For example, where a policy refers to an employee, the policy also applies to all contractors' employees, who are assigned with the responsibility of a KFU service as per contractual agreement.

The KFU information systems includes personal computers, laptops, servers, databases, networks, communication devices, applications, data stored in systems, data stored in internal and/or external medias, software and hardware licenses, copyrighted resources, technical and functional documents, confidential information such as root passwords and parameters, and all other information technology related assets that are owned or leased by the King Faisal University.

### *1.4 Owner and Custodian of this Policy*

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.

The original documents (including its version control) will be maintained under Quality Management Office (KFU-DIT-QMO) and all annexure to this policy manual will be available with the document owners of the specific item. Please refer to the 'document control' information of the document for point of contact reference.

All staff of KFU and other organizations, whose information security management has been included in the scope of this policy, shall be responsible for the awareness and strict implementation of this policy at their responsible area. It is automatically assumed, unless specifically identified and confirmed in writing, that all staff becomes the owner and custodian of the information assets in their control.

### *1.5 Glossary of Important Terms*

Please refer to Glossary of Terms relating to all policies and procedures available in the KFU website and this well help a reader to have an understanding of the important terms used.

http://apps.kfu.edu.sa/Glossary/Ar/glossaryofterms.aspx (for Arabic) and

http://apps.kfu.edu.sa/Glossary/En/glossaryofterms.aspx (for English).

### *1.6 Related References*

Relevant policies, procedures and/or guidelines must be referenced for a more comprehensive approach and understanding.

Interpretations and important rules that are applicable to public use shall be made available through the KFU-DIT's website: www.kfu.edu.sa/ar/Deans/it/Pages/Home.aspx (for Arabic) and www.kfu.edu.sa/en/Deans/it/Pages/Home.aspx (for English).

In addition to the above, the following policies shall be referred from the publications of concerned deanship/department of the KFU:

- Policies and procedures relating to HR and Contracted resources
- The consolidated regulations relating to various areas of concern as governed by the Legal and Administrative departments of the KFU.

### *1.7 Acknowledgement*

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

- COBIT Security Baseline from IT Governance Institute, USA, and their recommended control objectives (COBIT Release 4.1)
- ISO/IEC 27001:2005 standard
- Risk reviews and recommendations as obtained by the author of this policy manual, M. Shahul Hameed, MBA, M.Sc.IT, CMA, CIA, CISM, CGEIT, CISA, ISO27001LA, ICBRR, ITSM, PMP (initially as a consultant and then after assuming the responsibility of head of Quality Management Office under the deanship of IT), based on his industry based expertise.

## 2. Information Security Framework

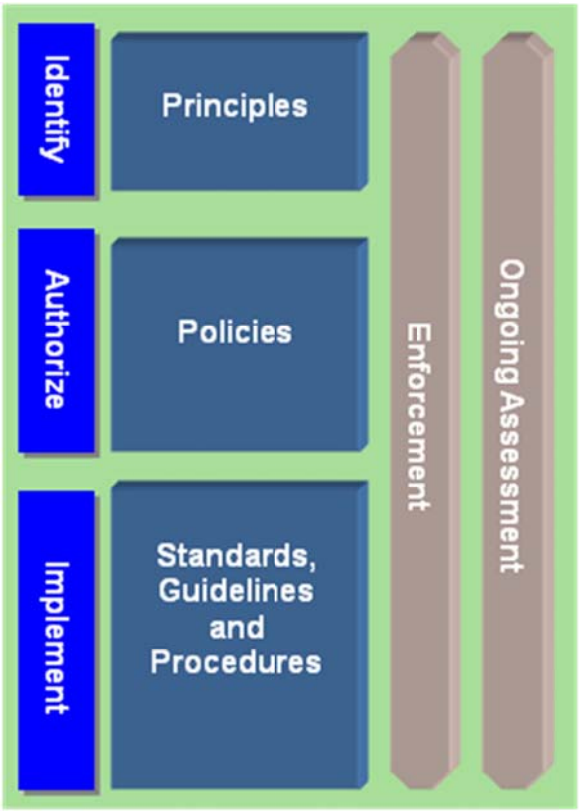
### *2.1 Policy Framework*

This policy is built on the best practices for Information technology security management for the purpose of security techniques and security requirements, as provided by British Standard (BS ISO/IEC 27001:2005) published on 18-10-2005.

Please refer to www.kfu.edu.sa/en/Deans/it/Pages/Resources.aspx for reading

***ISMS PDCA cycle – Plan-Do-Check-Act methodology for protecting the organizational assets***

### *2.2 Information Security Governance*



### *2.3 Information Security Baseline*

The overall business need in terms of security objective is met when:

- Information systems are available and usable when required, and can appropriately resist attacks and recover from failures **(availability)**;
- Information is observed by or disclosed to only those who have a right to know **(confidentiality)**;
- Information is protected against unauthorized modification or error, so that security, completeness and validity are maintained **(integrity)**;
- Business transactions and information exchanges between enterprises, customers, suppliers or partners can be trusted **(authenticity and non repudiation**).

And the Gaps in security are usually caused by:

- New vulnerabilities resulting from the widespread use of new technologies
- Lack of maintenance to assure all patches are made promptly
- Increased networking and mobile working
- Lack of security awareness
- Insufficient discipline when applying controls
- New and determined efforts of hackers, fraudsters, criminals and even terrorists
- Increased legislative, legal and regulatory security requirements

Therefore, the comprehensive body of this Information Security Framework and Policies and Procedures shall cover:

- Risk assessment approach, recognizing the risks and threats, treatment of risks and obtaining management approval of the proposed residual risks.
- Management Authorization to implement and operate this policy
- Coordination of all managerial efforts for the purpose of achieving the baseline objectives, as a minimum requirement, by organizing information security committee and authorize it to have all the resources and command accordingly.

### *2.4 Information Security Governance Committee*

A committee comprising of cross-functional senior management members shall be established in order:

- to ensure that there is clear direction and visible management support for security initiatives;
- To promote security within the organization through appropriate commitment and adequate resourcing, this includes investment in staff education, development and training.
- to give appropriate direction/approval/recommendations for physical and logical security management in order for use by those who are responsible for initiating, implementing or maintaining security in their deanship or department;
- to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings;
- to ensure that all such recommendations for standards be selected and used in accordance with applicable laws and regulations;
- To ensure continuous monitoring of security measures and facilitate appropriate risk management .

And this committee shall be called as “Information Security Governance Committee” and it can function in any of the following manner:

- By conducting formal and regular or special meetings in its name and with the scope of information security aspects only.
- By participating in the IT steering committee meeting, having all members included and the agenda will have information security as one of the key item of this meeting.
- By formal communication via email or other forms of written mails, clearly stating that the item discussed and decision made is of the information security governance committee responsibility.
- In whatever manner that the information security committee meetings are conducted, there should be considerable participation of the senior management.

### *2.5 Information Security Governance Committee Meetings & Proceedings:*

- The Security Committee will also convene, or include in the agenda of Senior Management meetings or IT Steering Committee meeting to be held at that time, whenever there is a significant change in scope or process or in the event of a significant security incident.
- In these meetings, the committee is responsible for reviewing the appropriateness of the Security Management Systems in meeting KFU needs and for the re-evaluation of the university's resources including information assets and a review of the perceived risks to those assets due to changes to the services.
- The committee decides on the assurance required from the controls and countermeasures implemented to manage each risk and hence the residual risks that are considered acceptable.
- The committee defines through policy statements and documented instructions, requirements for managing risks to the information used and gained in the execution of the critical Information and related technology services.
- The policies and instructions are translated into documented procedures that define how control objectives, controls and countermeasures are implemented by the 'owners' of the core and supporting processes to which they apply (i.e. the departmental managers having direct responsibility for the deliverables from the process). The process owners report to the Security Committee the continuing effectiveness of the actions taken to meet the policies.
- All process operators work in accordance with the policies and procedures and have a duty to report any deviations or incidents to their immediate supervisors using the incident reporting system currently in practice.
- Any suggestions or recommendations to improve the security control system will be made available to the security committee through the department/unit responsible. This may include existing or proposed controls/countermeasures and, wherever possible, alternatives and options for different degrees of assurance.

### *2.6 Information Security Governance Committee Members:*

Primary Members with decision making and approval authority for the purpose of distributing the policies as an interim measure until the policy is finally approved by the Board:

- The President
- The Vice President for Development and Community Services
- Representation of other vice presidents as nominated by the President
- The Dean of Information Technology
- The Dean of eLearning
- The Dean of Quality Assurance and Academic Accreditation
- Representation of other deanships
- Representation from Head of Quality Management Office of the Deanship of IT (for technical assistance)
- Representation from Finance, Security & Safety and Legal department (as and when required)

Other members (secondary) who can be called for supporting and facilitating the decision making of the above committee:

- Any other senior manager from Deanship of IT
- Disaster Recovery Center Manager (IT Production)
- Representative from Audit
- Other Representatives from Business Group(s)

## *2.7 Information Security Management Processes (ISMS)*

| ISMS Processes | Roles and Responsibilities of the Committee |
|---|---|
| Plan (establish the ISMS across all areas of concern) | Identification of information assets, risk assessment, identification of gaps in existing controls, and risk mitigation plan. Establish Security Policy, Control objectives, Processes and Procedures relevant to managing risk and improving security to deliver results in accordance with KFU's overall policies and objectives. (Head of Quality Management Office of the DIT to act as the coordinator between the committee and all responsible for the purpose of implementation). |
| Do (implement and operate the ISMS) | Implement and operate the Security policy, controls, processes and procedures through appropriate policy owners and responsible unit heads. (ISM will be the leader of the implementation of this policy). |
| Check (monitor and review the ISMS) | Assess and, where applicable, measure process performance against Security policy, objectives and practical experience and report the results to senior management for review. (Team work comprised of all DIT departments led by the KFU-DIT-QMO. Cooperation and support of other deanships for their network area is concern should be ensured) |
| Act (maintain and improve the ISMS) | Take corrective and preventive actions, based on the results of the internal and external audit checking for information security as well as for quality assurance objectives. Schedule and complete tasks to achieve continual improvement of the Security Infrastructure and Policies with the involvement of all stakeholders.<br><br>KFU-DIT-QMO to take the lead role for this act. |

## *2.8 Deliverables of the Information Security Management Process*

**Strategic Alignment:**

- Security requirements driven by KFU needs
- Security solutions cost-effectively fit for business processes

**Value Delivery:**

- A standard set of security practices and facilitate security awareness programs
- Properly prioritized and distributed effort to areas with greatest impact and business benefit
- A Continuous improvement culture

**Risk Management:**

- Agreed-upon risk profile
- Understanding of risk exposure
- Awareness of risk management priorities

**Performance Measurement:**

- Defined set of metrics
- Measurement process with feedback on progress made
- Independent assurance

## 3. Information Assets – Identification and Classification

### *3.1 Information Assets Database*

There must be a process and procedure to record, maintain and update a database of the organization's information assets.

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.

### *3.2 Information Classification and Protection Requirement*

Data and information classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored or transmitted. The classification of the data should determine the extent to which the data needs to be controlled/secured and is also indicative of its value in terms of Business Assets.

The term Business Assets, for the purpose of the scope of this policy, refers to any information upon which the organization places a measurable value. By implication, the information is NOT in the public domain and would result in loss, damage or even business collapse, was the information to be lost, stolen, corrupted or in any way compromised.

The following procedure should be followed for the purpose of data classification:

Computer output, regardless of media, which is classified in accordance with this classification scheme will be marked on the top and bottom of each page and/or on each output screen with the appropriate classification, except for the General classification, when it is created by the system.

**General ( " PUBLIC " )**

This classification includes all information that may normally be considered as General information, however, for business reasons management has determined that its use and dissemination needs to be controlled.

Shredding of this information is not required for disposal.

**Proprietary ( " FOR INTERNAL USE " )**

All data and information, except for media releases approved by management, used in conducting day-to-day business is regarded as proprietary and is not intended for discussion or disclosure to other than KFU authorized staff.

Shredding of this information for disposal is desired but not required.

**Restricted ( " PRIVATE " )**

Some of the data and information retained in the automated systems and on other media (e.g. microfiche, microfilm, and paper files) is critical to the organization. Other data and information is regarded as personal since it pertains to our employees, faculty and students. To provide adequate protection for this type of material it will be given a classification level of Restricted for identification.

Shredding of this information for disposal is required.

**Secret ( " CONFIDENTIAL " )**

This category of information includes KFU plans, the premature release of which could be detrimental to the university's strategic plan (e.g. acquisitions being planned/negotiated) or which could result in the filing of civil or other litigation). Also included in this category is any other information specifically designated as Secret by Senior Management of KFU.

This information is not authorized to be stored on any computer system except for desktop or laptop systems. When stored on desktop or laptop systems the information will be encrypted, using approved encryption software, to provide adequate protection. Additionally, this information will not be transmitted over any computer network within or between KFU community and other third parties, unless it is authorized and encrypted, using approved encryption software.

If this information is stored on removable storage media, then such items should be properly identified and stored in a locked desk drawer, cabinet or safe when not in use.

Shredding of this information for disposal is required.

Further detailed Guidelines for data classification and sensitivity shall be documented and communicated to responsible data/information owners and all support responsible in order that information receives an appropriate level of protection.

## 4. Risk Assessment

Due to the changing conditions in Information Technology and the evolving business needs of KFU and all its connected parties; threats to information and information systems increase.

This necessitates their periodic risk assessment. Risk Assessment identifies and quantifies the deviation from the implemented security mechanisms and controls, as well as the resulting risk. Risk management is an important issue for KFU and decisions must be reached either accepts risk or mitigates it to acceptable levels.

Risk assessment process should 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. Hence, this process must be completed in a coordinated manners and involving all the stakeholders including all deanships and departments, application systems owners, security analysts, operational risk specialists and quality management staff and other subject matter experts.

The detailed risk assessment methodology, policies and procedures shall be prepared in light of the best practices of the academic technology industry and applied accordingly.

Head of Quality Management Office of the Deanship of IT (KFU-DIT-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.

The QMO of the DIT (KFU-DIT-QMO), in coordination with the rest of the DIT departments and other deanships, shall develop an IT related risk management guidelines for continuously improve the risk management system applicable for protecting the information assets.

Periodical meetings (at least quarterly once) consisting of all coordinators shall be organized for active follow-up on unresolved items as identified during risk assessment and internal audits, and discussing remedial solution as well as further risk assessment planning.

# 5. Information Security Policy

## *5.1 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.

## *5.2 Approval of Policies and Procedures*

All policies on Information Security should be approved by the President or Vice President for 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.

The Dean of IT shall pass email or other form of written communication containing specific procedures or instructions or guidelines relating to information security control measure (preventive, detective and corrective controls), as an interim solution in case of its approval process will be delayed due to formalities to complete. Subsequent ratification by the competent authorities as per this policy shall be obtained by getting written approval or email confirmation or by resolving it through the Information Security Governance Committee periodical meetings.

## *5.3 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 the Head of Quality Management Office of the Deanship of IT.

### *5.4 List of Policies, Procedures, Guidelines and Checklists*

The Quality Management Office of the Deanship of IT, should 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.

## 6. Organization of Information Security Management

### *6.1 Internal Organization Policy*

In order to manage information security within the organization, a detailed information security organization structure must be documented, implemented and maintained.

The information security organization has been incorporated within the Deanship of Information Technology organization structure and special assignment within the responsibility of the Quality Management Office of the deanship.

Please refer to www.kfu.edu.sa/en/Deans/it/Pages/organization.aspx for more current as well as planned structure.

#### *6.1.1 Management Commitment*

| Role | Responsibilities |
|---|---|
| The President | Oversee overall "university security posture" (accountable to Board). Brief board, other stakeholders and public (press etc.) |
| Vice Presidents, Dean of IT and Information Security Governance Committee | Set security policy, procedures, program, and training.<br><br>Respond to security breaches and Responsible for independent annual audit coordination. |
| All other executive management | • Assessing the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of such information or information systems.<br>• Implementing policies and procedures that are based on risk assessment and cost effectively reduce information security risks to an acceptable level. Determining the levels of information security appropriate to protect such information and information systems.<br>• Periodically testing and evaluating information security controls and techniques to see they are effectively implemented.<br>• Seeing that the organization has trained personnel sufficient to assist the organization in complying with the requirement of this document and related policies, procedures, standards, and guidelines.<br>• Maintain the lists of accesses provided to the information assets for their respective teams.<br>• Seeing that all employees, contractors and others users of information systems are aware of their |

| | |
|---|---|
| | responsibility to comply with the information security policies, practices, and relevant guidance appropriate to their role in the organization. |

### *6.1.2 Information Security Coordinators*

Representatives from each department and deanships with relevant roles and job functions for

- Physical Security
- Logical security
- Systems, Data and network security
- Data and Systems business owners
- Procurement functions
- Change management functions
- Personnel security
- Legal and Compliance functions

Shall be designated and a comprehensive list be made available with the Quality Management Office of the Deanship of IT.

### *6.1.3 Information Security Roles and Responsibilities*

All information security responsibilities must be clearly documented and approved by the Dean of Information Technology. A formal procedure manual must exist as a baseline and the detailed roles and responsibilities including key performance indicators (KPI) need to be defined on the Job descriptions and the same must be accepted by both the employee and his immediate supervisor and approved by the next level of supervisor.

The following is the guidelines only and detailed functional responsibilities need to be covered on the job descriptions.

| **Role** | **Responsibilities** |
|---|---|
| Information Security Team | Lead the development and act as sponsor for ensuring appropriate security measures are consistent with organizational policy and maintained.<br><br>Responsible for overall policy implementation, adherence and awareness to users.<br><br>Facilitate development of security architecture for IT infrastructure Define assets identification and classification guidelines. |

| | |
|---|---|
| | Develop plans for risk assessment and mitigation.<br><br>Responsible for managing security incidents as per this policy<br><br>Manage third party access controls relevant to their area of concern |
| | Continued in next page… |
| **Role** | **Responsibilities** |
| Information Asset Owners/Custodians | Determine data classification levels for information assets so that the security organization can provide the appropriate levels of control to meet their confidentiality, integrity and availability requirements. |
| Information Security Coordinators | Undertake the coordination as required between the rest of the members of their group/department with the information security department (i.e. security process owners) for the purpose of creating awareness, enforcement of information security policies and procedures, and incident reporting. They also play vital role in the monitoring and evaluation of information security controls implementation and would be provided appropriate level training for effectively performing their role. |
| Security specialist / advisors | Promulgate and assist with the design, implementation, management and review of the organization's security policy, standards and procedures. |
| IT developers | Implement information security in products and applications they develop and install. |
| IT testers | Ensure Generic security controls as well as specific security controls as required per application based requirement description, have been tested properly during all stages of System Integration testing as well as User acceptance testing. Ensure security of information and information systems made accessible to them for the purpose of testing. |
| Users | All employees and staff from outsourced contracts, faculty, students and, where relevant, third-party users share responsibilities for the security of information systems accessible to them , including<br><br>• Awareness of the information security policies, practices, |

| | |
|---|---|
| | and relevant guidance appropriate to their role in the organization.<br>• Compliance with the security policies and procedures related to the information and information systems they use.<br>• Reporting of vulnerabilities or incidents affecting security or security policy compliance to the appropriate management channels and keeping virus vaccine signatures up to date |
| IS Auditors & Quality Assurance Auditors | Provide independent assurance to management on the appropriateness and effectiveness of the information security objectives. |
| | Continued in next page… |
| **Role** | **Responsibilities** |
| Information Security Governance Committee | Individuals representing various management levels should meet as a committee to discuss the security program and offer suggestions on how security can be implemented within their respective domains to enforce the policy with minimal impact on functionality. Regular minutes of the meeting need to be recorded with action items that are reviewed at each meeting. (Please refer to section 2.4, 2.5 and 2.6 of this policy manual for more details). |
| Information Security Management (ISM) | Information security management is comprised by management staff of the IT security as well as IT governance responsible under Quality Management Office of the Deanship of IT. Involved in the complete execution of planned and approved policies and procedures implementation including monitoring and evaluation of the implemented controls and reporting the same through the Dean of IT to the Information Security Governance Committee. |
| IT Governance under the KFU-DIT-QMO | Working in close relationship with IT Security team and rest of the process owners within IT and the business owners, |

| | |
|---|---|
| | establish and ensure implementation of the IT policies, processes, procedures, quality standards, and organizational structures designed to provide reasonable assurance that the business objectives are achieved in secured manner.<br><br>To monitor and evaluate the key performance of the defined processes within IT and lead the control activities in accordance with the set standards. |

### 6.1.4 Authorization process for Information processing facilities

All purchases of new systems hardware or new components for existing systems must be made in accordance with this information security policy as well as in compliance to the university's other policies relating to procurement, finance and administrative management areas concern.

IT steering committee and procurement management committee are the management tools for major decision making as well as follow-up on the strategic plans.

All requests to purchase must be based upon a business case and requirements specification document and take account of longer term organizational business needs. This document must have senior management approval.

Except for minor purchases and purchasing for emergency fixing for the purpose of business continuity, in which case it will be from the existing support contractor or supplier and relating to the existing configuration and the equipment; all systems must be purchased through a structured evaluation process which must include the development of a detailed Request for Proposal (RFP) document. Information security requirements must be identified within the RFP.

All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Information security requirements for new installations are to be circulated for comment to all interested parties well in advance of installation.

All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the live environment.

The development of bespoke (made to measure from the scratch as against customization of the standard packages) software is only to be considered, if warranted by a strong business case and supported both by management and adequate resources over the projected life time of the resultant project.

### 6.1.5 Confidentiality Agreements

A breach of confidentiality is usually a disclosure of information. It must be considered as an information security incident and treated accordingly. (Please refer to 13.2 Management of Information Security Incidents and Improvements in this manual).

Breaches of confidentiality, including the one arising from a breach of an employee's terms and conditions of employment, and from non-compliance with Non-Disclosure

Agreements, must be reported to the ISM as soon as possible. A Non-Disclosure Agreement template shall be made available on the website.

### *6.1.6 Contact with Authorities*

All contact with government or regulatory authorities shall be based on the communication policy of the university and must be authorized by the president or vice president relating to the area of concern. All needed staff members must go through their department head or the dean for finding out the approved contact and protocol for such kind of external communications.

### *6.1.7 Contact with special interest groups*

All contact with special interest groups, relating to information security and information technology, and only during the process of meeting KFU's business objectives, shall be authorized by the Dean of Information Technology on case to case basis. All heads of departments within the DIT are authorized for contacting special interest groups relating to job practices area of concern.

### *6.1.8 Independent Review of Information Security*

KFU's Deanship of Quality Assurance and Academic Accreditation (QAAA) shall lead the process of independent review of the information security. However, the Dean of IT, through the coordination of Quality Management Office (QMO), shall arrange to have the independent review based on vulnerability assessment, ethical hacking, and security reviews to be conducted by the subject matter experts.

It is also assumed that all external audits and regulatory compliance audits will provide reasonable independent review and recommendations accordingly.

## *6.2 External Parties Policy*

High level of security control measures must be ensured to maintain the security of the KFU's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

Consideration of such controls must focus on the following critical areas of concern:

- Identification of risks for providing access to the KFU's information assets to external parties and implementing adequate level of controls before granting such access.

- All identified security requirements must be addressed before giving customers to have access to the KFU's information or assets.
- Addressing security in third party agreements

## 7. Asset Management Policy

### *7.1 Responsibility for Assets – Inventory Control*

There must be a process and procedure to record, maintain and update a database of KFU's and its associated sites all information assets.

Information assets include information (data and/or collection of data in electronic and paper form), hardware, software, infrastructure, network links, people, physical items, university's image and reputation, processes and services required to support the business; and identified during the risk assessment process as assets that need to be protected.

An asset register template shall be published on the KFU website or its intranet for each department/deanship to follow for updating the information.

### *7.2. Responsibility for Assets - Ownership of Assets*

All information and assets associated with the information processing facilities must be owned by a designated part of the KFU and/or its affiliates.

A detailed sub policy or procedure with required controls information shall be defined and published on the KFU website and/or intranet network.

### *7.3. Responsibility for Assets - Acceptable Use of Information Systems*

A detailed sub policy covering the rules for the acceptable use of information and assets associated with information processing facilities should be documented and implemented.

Please refer to KFU-DIT-ISP-07-3-AUP Acceptable Use Policy 2011 v1.0.

# 8. Human Resources Security Policy

## *8.1 Prior to employment*

### *8.1.1 Roles and Responsibilities*

All employees, contractors and third party users should be made to understand their responsibilities. Prior to employment, the administrative responsible for recruitment as well as the deans and department heads, who required the human resources, should ensure that a selected candidate for a particular function or processing area is suitable for the role they are considered for and appropriate care must be taken to reduce the risk of theft, fraud or misuse of facilities by strict enforcement of the below given controls.

Detailed guide books for recruitment and staff induction process as well as the job descriptions per role shall be prepared and approved by concerned authorities. These guides should be published.

### *8.1.2 Screening*

Policy and/or procedure concerning the Human Resources (HR) recruitment process must address rules and control requirements demanding background verification checks on all candidates for employment, contractors, and third party users.

### *8.1.3 Terms and conditions of employment*

Information security responsibility of each employee must be addressed in the respective employment contract. HR recruitment policy and the employment contract template need to be reviewed and updated to include this security control requirement.

## *8.2 During Employment*

### *8.2.1 Management Responsibilities*

All deans and management of departments must require all employees, contractors and third-party users, who are working under their area of concern, to apply security in accordance with established policies and procedures of the organization.

All critical job descriptions must clearly address the security responsibility in detail and also by providing the reference to the relevant policies and procedures.

### 8.2.2 Information Security Awareness Education and Training

All employees and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates should be made in all relevant policies and procedures, including job descriptions.

Personnel has to be adequately informed and updated on threats and risks on information and information systems, as well as on principles, policies, procedures and security mechanisms implemented by KFU.

All employees must understand the need for protecting corporate information and perform their day-to-day work adhering to this information security framework and policies defined by KFU. It is imperative that all new employees, as part of their orientation training, are made aware of the information security standards of KFU. They should be made aware of the agreements and contracts signed with regard to their roles and responsibilities of information security.

This awareness training can be in the following forms:

- Formal trainings and/or workshops as coordinated by centralized KFU responsibility for HR Training and to be conducted by the ISM management under the QMO of Deanship of IT.
- Information printouts or email communications to all relevant parties
- External trainings and other forms of training as per KFU training policy
- Department briefing, where the minutes of the meeting should be formal and a copy of the report should be sent to QMO of the Deanship of IT for filing for future reference and auditing.
- ISM under the QMO of Deanship of IT should prepare an annual awareness training plan and execute it.

### 8.2.3 Disciplinary process against a security breach

Disciplinary action shall be taken in accordance with the KFU HR policies, procedures, guidelines and instruction booklets, memos regarding the Human Resources administration and management.

All employees and contracted resources, who have committed a security breach should be asked to give a written explanation for his failure to adhere to the Information Security policy as well as for his lacking good ethics and code of professional conduct.

The KFU management may apply discipline sanctions against the employee for any misconduct on the part of the employee. The dean or department manager need to solve such issues at their level first in consensus with the concerned employee. KFU HR to intervene in case the issue is not resolved. KFU HR has the authority to

administer sanctions against an employee as per its rules for "Violations and Penalties".

All security breach of contractors and third-party users shall be treated with the disciplinary process as per the KFU's legal procedure and the terms and conditions as mentioned in the applicable contracts will also be used in support of the legal proceeds by the KFU.

### *8.3 Termination or change of employment*

**Security Violations Resulting in Instant Termination:**
All employees or contracted resources, who have stolen KFU's property or have given false personal data (e.g. regarding their educational background) or do not conform to the security policies and procedures of the Company, must be immediately dismissed. In such cases criminal prosecution must be considered, too.

All deans and department heads are responsible for ensuring that employees, contractors and third party users exit KFU or change employment in an orderly manner.

All such responsible activities must be performed in coordination with KFU administration department (responsible for HR) and care must be taken on the following:

- All employees, contractors and third party users should return all of the KFU assets in their possession upon termination of their employment, contract or agreement.
- All the access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination or their employment, contract or agreement, or adjusted upon change.

**End of Employment**
Right after an employee's employment term ends for any reason (involuntary contract termination, voluntary departure, contract termination with mutual consent) the KFU HR administration department in cooperation with the employee's immediate supervisor are responsible for:

- Revoking all logical and physical privileges granted to the employee.
- The return of all KFU information or property in the custody of the employee.

Additionally, it is the employee or contractor's immediate supervisor's responsibility to have the employee collects their personal belongings before he leaves.

In case where an employee has given notice of his departure and is on leave until the last day of his employment, then the above actions must take place right after his leave starts.

Policies relating to Chapter 9 (of this ISP manual) 'Physical and Environmental security' and '11 Access control policy' (with special reference to user management policy, mobile computing and teleworking policy) need to be considered prior to completing the end of employment process.

**Transfer of Employees Intending to Depart**

The KFU HR administration manager in cooperation with the relevant Department Manager or the dean must, if deemed necessary, make sure that employees who hold important positions (e.g. handling sensitive information) and have given notice of their intention to leave the employment of the Company, must be transferred to positions from which they can cause minimum harm to KFU's assets. Alternatively, it is up to their Manager to give them mandatory leave.

**Return of Information Assets and Company Property at the End of Employment**

At the end of their employment term, employees must not retain or remove from the KFU premises any corporate information. All information kept by the employee during his employment must be returned to the employee's immediate supervisor before departing.

They must also return all property belonging to the KFU and have been issued to them to perform their duties such as portable computers, software, mobile phones, keys, manuals etc.

**Exception:**

Exceptions to the above rule include personal copies of information disseminated to the public and personal copies of correspondence and documents relating to the terms and conditions of their employment (e.g. the employment contract).

**Notification Responsibility for Employee Job Duty Changes**

The Human Resources Administration Manager in cooperation with the user's supervisors must immediately inform the ISM (Information Security Manager working under the Quality Management Office of the Deanship of IT) about internal employee transfers or job duty changes, so that all necessary measures are taken with regard to the revocation or change of access rights to corporate information and systems.

Any relevant information relating to the Safety & Security department must also to be sent to them directly for taking care of their authorization and monitoring to the facilities of KFU.

## 9. Physical and Environmental Security Policy

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

Refer to www.kfu.edu.sa/en/Departments/Security_safety/pages/departments.aspx

In addition to this, Information security policy recognizes the additional care and protection need to be ensured on the information and information processing facilities, including the systems at the Disaster Recovery center.

The ISM in coordination and support by Department of Security and Safety shall develop and publish a detailed sub policy guidelines and procedures in order to implement the needed controls. Such sub policies must include, but not limited to:

- The physical security and environmental controls that must be established in alignment with the risk assessment and in consultation with the asset owners/custodians.
- Physical security perimeter defined for areas that contain information and information processing facilities
- Physical entry controls for the secure areas within the defined security perimeter
- Securing offices, rooms and facilities
- Protecting against external and environmental threats
- Physical protection and guidelines for working in secure areas
- Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible isolated from information processing facilities to avoid unauthorized access.

Security controls need to be identified and implemented for covering Equipment security, which should address:

- Equipment siting and protection from environmental threats
- Equipment protection from power failures and other disruptions caused by failures in supporting utilities
- Protection for power and telecommunications cabling carrying data or supporting information services from interception or damage.
- Equipment maintenance
- Security of equipment at off-site premises such as Disaster Recovery center and critical servicing locations
- Secure disposal or re-use of equipment
- Authorization for removal of equipment, information or software

## 10. Communication & Operations Management Policy

### *10.1 Operational procedures and responsibilities*

#### *10.1.1 Documented Operating Procedures*

All critical information processing systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organization's information security.

It is the responsibility of IT production (systems administration, network management and operations management responsible) to have the list of all critical and sensitive application systems and the operating systems where the application system is hosted. Then, all systems referred in the list need to have an adequate level of operating procedures documented, maintained and made available to all users on need to have basis.

Access to Operating Systems manufacturer supplied user guides and technical manuals need to be referred appropriately for quick reference when needed. A quick reference guide to the comprehensive and compiled version of all such relevant technical manuals must be made available to the all the system and network operators and their immediate supervisors.

All technical manuals, including those relevant for the 'in-house' designed application systems, are mandatory for the information processing management.

A check list based on the list of application systems should be prepared to contain the information as to the availability of technical manuals and the last updated status as compared to last version of the current package running in production.

System owners are responsible to ensure the availability of technical manuals, updated to the recent version implemented and any gap to this need to be informed to the business owner of the application system in order for accepting the risk.

#### *10.1.2 Change Management*

All changes to information processing facilities and systems must be fully tested and approved, by competent authorities, before being implemented.

It is to be understood that all kind of alterations that require changes to hardware, software, networking, infrastructure, data structure, and rules for manual controls or schedule of processing relating to information processing system, would introduce a new risk. Therefore, appropriate risk assessment must be conducted by competent

personnel or department for advising the change management responsible for taking appropriate counter measure for any identified risk.

Detailed change management procedures with robust controls should include the following rules:

- Change management process should ensure that an acceptance criteria was established in coordination with the business (refer to section 10.3.2 System Acceptance of this policy manual) used for scope verification of the project.
- Emergency changes to the systems, applications and/or data may only be used in extreme circumstances and only in accordance with emergency amendment procedure.
- Version control procedures should always be applied.
- Patches to resolve software bugs may only be applied where verified as necessary and with management authorization. They must be from a reputable source and are to be thoroughly tested before use.
- Upgrades to software must be properly tested before they are put into live environment
- Acceptance testing should be carried out in accordance with section 10.3.2 System Acceptance of this policy manual and related testing guidelines and procedures.
- A change management committee or change advisory board must be organized and detailed procedure or guidelines for its function must be developed and
- maintained.

### *10.1.3 Segregation of Duties*

Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Therefore, the techniques of dual control and segregation of duties are to be employed to enhance the control over procedures wherever both the risk from, and consequently impact of, a related information security incident would likely result in financial or other material damage to the organization.

ISM (Information Security Management) should create periodic awareness (at least once in a year) among all critical management staff and their subordinates on effective implementation of segregation of duties in their respective departments/deanships or functional area.

### *10.1.4 Separate Development, Test and Production facilities*

There must be separation in the environments of development, testing and production of the information systems. This separation must be implemented at the

physical level using different information systems and infrastructures. The development and upgrade of information systems and applications must always be conducted in a development and testing environment and then be incorporated into the production environment.

**Exception:**
An exception to this policy is allowed when the absolute logical separation of the development and testing environment from the production environment is achievable at the operating system level (e.g. using virtual servers).

### *10.2 Third-party Service Level Management*

Information Security management (ISM) must ensure that the security controls, service definitions and delivery levels included in the third party service delivery agreement.

A control procedure, including providing standard template for SLA (Service Level Agreement) incorporating adequate level of security requirements of KFU and check list for ensuring that such controls are properly implemented, operated and maintained by the third party.

The minimal contents of the SLA should address the KFU's business need of the following:

- Availability, reliability, performance, capacity for growth
- Levels of support provided to users
- Continuity planning, security
- Minimum acceptable level of satisfactorily delivered system functionality
- Restrictions (i.e. limits on the scope – amount of work)
- Service charges
- Central processing point and print and distribution procedures, if applicable
- Change Management procedure

Further, the SLA should include the right of KFU appointed audit in order to ensure that KFU's security requirements are adequately met by the third-party service delivery management.

There should also be a clearly defined procedure identifying the roles and responsibility for efficiently and effectively monitoring and reviewing regularly of the services, reports and records provided by third party. Minimum frequency of such kind of review should be monthly.

## *10.3 System planning and acceptance*

### *10.3.1 Capacity Management*

The Deanship of IT's management process should ensure that the business needs are identified regarding availability and performance of information services and this should be converted into measurable key performance indicators (KPI).

Such identified and agreed KPIs should be integrated with the higher management follow-up as well as linked to KFU HR Administration policy on its performance appraisal process.

KFU's DIT Internal meetings would monitor and control on the identified and agreed KPIs on each meetings periodically (at least quarterly once).

DIT management should ensure that appropriate modeling tools are used to produce a model of the current system which has been calibrated and adjusted against actual workload and is accurate within recommended load levels. Modeling tools should be used to assist with the prediction of capacity, configuration reliability, performance and availability requirements.

DIT management should also ensure that in-depth technical investigations be conducted on systems, at least once in two years time, hardware; and should include forecasts concerning future technologies.

### *10.3.2 System Acceptance Criteria for development and testing*

Formal acceptance criteria for new information systems, upgrades, and new versions should be established in order to use the same as the baseline for the purpose of designing and testing prior to rollout to production. The change management process should cover this basic requirement in their checklist as one of the critical item in the flow of processes involving the changes to the business processing.

The Information Owners should set the acceptance criteria for the information system, in cooperation with the IT Systems Development (Application support and/or Oracle and/or Internet departments) through the IT business relationship management as coordinated by the Quality Management Office of the deanship of IT.

The acceptance criteria must be clearly defined, documented and approved by all involved parties.

**Testing of the systems**

Management must ensure that changes are tested in accordance with the impact and resource assessment in a separate test environment by an independent (from developers) test group before moving into production environment. Back-out plans should also be developed.

Acceptance testing should be carried out in an environment similar to the production environment (i.e. similar security, internal controls, workloads, etc.). However, in case of any capacity or workload differences due to technical constraints, then this must be reported as part of the comment on the test report, so that the business owners and the change management advisory board understand and may accept the residual risk exposed therein. (Please refer to section 10.1.2 Change Management & section 12.1.2 SDLC methodology of this policy manual.)

### *10.4 Protection against Malicious and Mobile code policy*

To protect the integrity of software and information, adequate level of controls need to be identified and implemented. Such controls include:

- Detection, prevention, and recovery controls to protect against malicious code
- Appropriate user awareness procedures
- Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.

Please refer to Chapter 7 section 3 (Acceptable Use Policy) where particular reference may be made to its section 5.4 Unacceptable Use and 5.10 Mobile Computing / Teleworking and Using them in public places.

### *10.5 Backup and Recovery Policy*

DIT management should implement a proper strategy for back-up and restoration to ensure that it includes:

- Periodical review of business requirements (at least once a year)
- Development, implementation, testing and documentation of the recovery plan
- A checklist and procedure to ensure that backups are satisfying the above mentioned requirements, which include periodical testing of backed up data for evaluating the quality of data retention.

A clearly defined procedure, including automated scripts implemented at each critical systems for the purpose of backup copies of information and software on regular

interval; should be made available to the operations management (IT production – i.e. Systems & network operation department of the DIT) as well as at the DRC (Disaster Recovery center).

The check list template should cover the following minimum content:

- 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.

In case of the DRC is outsourced, an appropriate arrangement to incorporate the information security requirements on the service level agreement must be made. Adequate level of encryption to critical data must be considered. KFU should have an audit right of the DRC arrangement as provided by the service provider.

### *10.6 Network Security Management Policy*

**This portion of the policy is for "Internal Use" only. All authorized users are requested to contact shahul@kfu.edu.sa, the head of Quality Management Office, for the copy of this portion.**

### *10.7 Media Handling Policy*

Information security issues need to be considered in the management of removable information and related technology media. Media (communication) tools are used to store and deliver information or data. Confidential data may be revealed to unauthorized persons from discarded consumables, e.g. discarded draft printer output, CDs etc.

Therefore,

- All storage media (such as hard disk drives, CD-ROMs, DVDs, or any other kind of removable storage media), printouts, manuals and generally information in printed form containing sensitive information, must be physically secured in locked drawers and cabinets when not in use. This includes securing them during non-working hours. The protective measures must vary according to the criticality of the information assets. Protection and disposal of all the information assets of the KFU should be as warranted by the classification of the respective information asset.
- The information systems and the storage media that no longer meet business needs must be physically destroyed in a secure manner.
- Rewriteable media must first be erased using a secure procedure (e.g. through multiple overwrites).
- Paper documents containing sensitive and critical information must be destroyed using paper shredders.
- Special attention should be paid to storage media as well as paper documents that are collected for destruction in a central location (e.g. they should be kept in a security cabinet)
- All the mobile storage media (e.g. CDs, memory sticks, other kind of removable storage media, etc) must be checked for malicious software before use.

Further, information security management in coordination with IT Operations and Technical support department should ensure that:

- Only personnel who are authorized to install or modify software shall use removable media to transfer data to / from the enterprise network.
- Any other user should be asked to justify the business need and authorization should be provided from the deanship or department head and approved by the Dean of Information Technology.
- List of users with such kind of exception should be prepared and sent to Quality Management Office of the Deanship of IT, who are responsible for IT governance.
- Appropriate risk mitigation measure must be identified and implemented against the risks associated with the following:
    - Portability of the media from one area to another area

- Loss or 'disappearance' of media, which could compromise the confidentiality of the KFU's data
- Damage to media, which could compromise the integrity of corporate records.

## *10.8 Policy for Information Exchange*

### *10.8.1 Information Exchange*

Sensitive or confidential data / information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured.

There should be a clearly defined formal exchange of data/information procedures, and controls in order to protect the exchange of information through the use of all types of communication facilities.

### *10.8.2 Exchange Agreements*

Appropriate service level agreements with adequate level of security controls should be established for the exchange of information and software between the organization and external parties.

### *10.8.3 Transportation of Media*

The designated owners of documents or any kind of media(s) that contain sensitive information are responsible for ensuring that the measures taken to protect their confidentiality, integrity and availability, during and after transportation, transmission, are adequate and appropriate.

### *10.8.4 Electronic Messaging*

All sensitive and confidential information passed through electronic messaging system must be sent as an attachment of protected (password or encryption) file rather than sending as the text part of the message itself.

### *10.8.5 Interfaces and interconnection of business information systems*

Detailed policies and/or guidelines and/or procedures should be developed, implemented and maintained in order to protect information associated with the interfaces among different application systems.

For example, a classified data set from one application might be passed via an interface to another business application, where the same level of security classification of data has not been done and this will leave the KFU at risk of compromising the security controls via back door.

### *10.9 Electronic Commerce services policy*

Security of electronic commerce services and their secure use is of paramount important for KFU and its community, where this service is used. A detailed policies and procedures must be developed, implemented and maintained for all applicable electronic commerce services that KFU and its affiliates are engaged in, with due attention on the following controls:

- Electronic Commerce: Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification;
- On-line transactions: Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized message duplication or replay; and
- Public available information: the integrity of information being made available on a publicly available system (web site) shall be protected to prevent unauthorized modification.
- The KFU's web site is an important information resource for the whole KFU community and its safety from unauthorized intrusion is a top priority. Therefore, web sites may only be developed and maintained by properly qualified and authorized personnel. All changes to the web site must be documented and should be processed through Change Management process before making the change.
- Access to the internal network must be protected from access via the web server
- Appropriate warning message must be provided on the web site that no information may be copied and reproduced without elementary copyright notices.
- Staff authorized to make payment by credit card for goods or services ordered on the Internet, are responsible for its safe and appropriate use.
- Web browsers are to be used in a secure manner by making use of the built-in security features of the software concerned. Management must ensure that staff is made aware of the appropriate settings for the software concerned.
- Information obtained from Internet sources should be verified before used for business purposes.
- All eLearning processing systems including the www.kfu.edu.sa web site need to be designed with protection from malicious attack given the highest priority.

### *10.10 Monitoring Use of Information Processing Facilities Policy*

**This portion of the policy is for "Internal Use" only. All authorized users are requested to contact shahul@kfu.edu.sa, the head of Quality Management Office, for the copy of this portion.**

## 11. Access Control Policy

KFU's primary objectives to safeguard information against unauthorized use, disclosure, modification, damage or loss is enabled by preventive and detective controls, which includes provisioning and monitoring of physical and logical access controls that ensure access to the systems, data and software is restricted to authorized users only.

Effective access control policy, therefore, need to consider:

- Authorization, authentication and access control
- User identification and authorization profiles
- Need-to-have and Need-to-know principles for providing access rights
- Strong authentication controls for all remote accesses including WAP.
- Centralized security administration
- And implementation of an effective monitoring of the above

### *11.1 KFU requirements for access control*

#### *11.1.1 Access control policy*

A detailed access control procedures, guidelines and checklists need to be documented, implemented, and reviewed periodically based on KFU security requirements for access. The periodicity of reviewing and maintaining the access control policies and procedures should be strictly in correlation with the critical changes to the application systems involved, changes to location, infrastructure and regulatory compliance requirements.

The Information Security Management (ISM) should ensure implementing controls for periodical obtaining of the entitlement list for access from business owners and getting it reassessed to reflect changes to the roles and responsibilities.

The information systems owners (i.e. the deanships or departments responsible for a particular and critical information systems. Example: Deanship of Registration for the Banner Students Registration system) should be reviewing periodically the "Access Profiles" created for each category of their respective business application function for the purpose of verifying the effectiveness of controls implemented for segregation of duties and the access privileges associated per job roles.

Immediate implementation of corrective actions, if needed, must be ensured by the business owners.

## *11.2 User Access Management*

### *11.2.1 User registration*

The access control procedure should cover the detailed steps ensuring timely action in relation to requesting, establishing, issuing, suspending and closing user accounts.

For all systems and applications under production environment, user ID creation/deletion/modification or privileges should be done only by IT security.

All the above mentioned actions should require formal approval and a standard access control registration form (single form covering all application systems or a separate one for each identifiable application or group of applications) should be designed and used. Usage of an intranet application or integration of a work-flow processing under the KFU's HRMS (or email) system can be used for this purpose.

When employees are given their user-id/account, they should be provided with initial or refresher training and awareness on information security issues. Users must be asked to review a set of rules and regulation for system access periodically (at least twice a year).

Additional care must be taken when granting access or facilitating WAP connection to any users. Please refer to section 11.4 Network Access control of this policy manual.

Arrangements involving third-party access to IT facilities must be based on a formal contract containing or referring to all of the necessary security conditions to ensure compliance with the KFU's security policies and standards.

Third-party users should not be provided with user codes or passwords unless they have signed a nondisclosure agreement.

All third-party users are provided with the relevant security policy and related documents and must be asked to sign off that they understand their obligation.

The granting of access, changes to existing access rights and removal of access are authorized by the appropriate system owner taking into account least privilege, segregation of duties and the level of access required.

Business users should not be granted access to development and test systems except where specifically required for user testing.

Segregation of duties principle must be strictly adhered when granting access rights to Development users. They should not be granted access to production except where specifically required for trouble-shooting or support reason, where such kind

of access right is allowed only for the period of such kind of service is required and the same can be supervised by the system owner.

The definition of emergency situation, for the purpose of granting access to abnormal profiles (such as development or support engineer getting access to production system), and the action that must be taken is provided by the system's business owner, who should ensure that individuals to whom emergency access rights can be given are nominated in advance, that emergency rights are removed as soon as the emergency is resolved and that all actions are logged.

### *11.2.2 Privilege Management*

Privilege is the term used throughout most applications and systems to denote the level of operator permission, or authority. For example, read only access, permission to create only, permission to change only, permission to all kind of updating etc.

Privileged users are allocated with powers of functionality significantly greater than those available to the majority of users. For example, system administrator, network administrator, database administrator, security administrator etc. In certain systems, they are called as 'super user' and in others as 'root user'.

The allocation and use of privileges should be restricted and controlled in one of the following ways:

- Access to all systems must be authorized by the owner of the system and such access, including the appropriate access rights (privileges) must be recorded in an access control list. Such records are to be regarded as highly confidential documents and safeguarded accordingly.
- Allocating inappropriate privileges to inexperienced staff can result in accidental errors and processing problems, and therefore, this practices should be prohibited
- User IDs which suggest their privileges (e.g. user id of 'master or admin' may invite hackers to try hard to crack their password. Therefore, user ids of the application systems should avoid such kind of leading ids.

### *11.2.3 Password Management*

All business critical application systems must be forcing the users to apply quality passwords, explained as below:

- Enforcement of initial password change on first use
- Appropriate minimum password length ( 8 characters)
- Appropriate and enforced frequency of password changes (45 to 60 days)

- Password validation against list of not-allowed values, history tables; and
- Adequate protection of emergency passwords

### *11.2.4 Periodical Review of User Access Rights*

All access rights must be reviewed periodically to confirm they are still as granted and that they correspond to the user's and KFU and/or its related concern's business needs.

All users should be asked to control the activity of their accounts by reviewing login times. Any abnormal activity must be reported in a timely manner.

Detection of unauthorized changes to access rights in a timely manner should be conducted and the procedure, besides implementing possible automated control procedure, need to have the following manual control practices:

- System owners/Security administrators should arrange to take out the user accounts list from all critical application systems
- Clean up the access control lists by removing all terminated/resigned users by reconciling with the list of employees as per HRMS
- Arrange to sort the listing per department and deanship and send the same to the dean or department head for his Managerial Review and Confirmation of the list of users and their profile, by giving appropriate time notice to reply (three weeks maximum).
- In case of no response within this time, then to escalate this security requirement to higher level of authorities
- Keep QMO of the DIT with a copy of all such correspondences for IT governance.

## *11.3 User Responsibilities toward access control policy*

- Users must follow good security practices in the selection and use of quality passwords (See section 11.2.3 above for quality passwords).
- All users must check the activities of their accounts as reported by the system, i.e. last login times etc., and report in a timely manner if any abnormal activity found
- Users must ensure that unattended equipment has appropriate protection
- Users must ensure that they receive the latest updated version of Acceptable Use policy and strictly follow the same.

Please refer to KFU-DIT-ISP-07-3-AUP Acceptable Use Policy 2011 v1.0.

### *11.4 Network access control*

Network infrastructure is very critical asset of KFU and all the authorized external network connections. Using network infrastructure, besides the great advantages their development and usage provide, also poses serious risks to the security of transmitted data and information systems.

A detailed policy, procedures, guidelines and checklists, therefore, need to be established, implemented and maintained. These set of policies and procedures also depend on the configurations of the resources and the threats exposed by each item of the infrastructure.

All established policies relating to network infrastructure must be implemented in all networks, including LANs (Local Area Network), WANs (Wide Area Network), WAPs (Wireless Application Protocol), and also network services leased from third parties. The policy must refers to all the equipment the KFU network infrastructure consists of, including hardware and software.

In particular the following issues are addressed:

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

The Related procedures and guidelines are valid and must be applied as a part of this policy, which should be based on the following principles:

- Access to the resources on the network must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.
- The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and range of privilege restrictions.
- All those staff responsible for the network and external communications is to receive proper training in risk assessment and on how to build secures systems which minimize the threats from cyber crime.
- It is a priority to minimize the opportunities for cyber crime attacks on the organization's systems and information through a combination of technical access controls and robust procedures.

- Contingency plans for a denial of service attack are to be maintained and periodically tested to ensure adequacy.
- E-commerce processing systems including the web site(s) are to be designed with protection from malicious attack given the highest priority.
- E-commerce related web site(s) and their associated systems are to be secured using a combination of technology to prevent and detect intrusion together with robust procedures using dual control, where manual interaction is required.
- An access control list must be maintained and updated regularly. This list must be classified as highly confidential and protected accordingly.

In addition to all applicable controls for network access as given above, all wireless access facilities should have minimum the following controls:

- The wireless network should be isolated in a separate network protected with a firewall and IPS.
- Physical access to the WAPs should be protected.
- The wireless network ID should not be broadcasted.
- Access to the WAP network should be password protected in compliance with the KFU's password policies (Please refer to 11.2.1. user registration of this policy).
- IT security should ensure that all communication across the WAPs should be encrypted with a strong encryption algorithm as recommended by industry standard best practices.

### *11.5. Operating system access control*

Operating System security parameters based on KFU and/or vendor's recommended standards, must be installed on all systems. Deviations to this need to be approved formally after assessment of compensating controls.

All systems require a user identifier and user authentication mechanism to allow access.

Systems should validate the user identifier and user authenticator combination as a pair and reject the logon attempt if it is invalid. Systems should not inform the user which of the two is wrong.

Implementing control practices of central identification and access rights management to prevent unauthorized access to operating systems will help ensure security profiles assigned by multiple security or system administrators involved are consistent.

Therefore, system access should be centrally managed to ensure consistent user profiles for all systems. Users are to be identified and assigned authorizations in a standard and efficient manner, preferably using a centralized user management process and system.

Information security management should keep in their mind that a single sign-on is required for all required resources. Information technology management planning should apply this requirement in all such upgrade or replacement plans of the systems.

Following a system failure, users are not to be allowed back on the system without re-authentication.

## *11.6 Application and information access control*

### *11.6.1 Information Access restriction*

Unauthorized access to programs or applications could lead to fraudulent transactions or false entries. The integrity and stability of the organization's databases must be maintained at all times. For this, it is very important to implement information access restrictions through the application control and the database control should not allow any changes or updating unless it is through application controls.

All data must be periodically cleansed, through the business users using application interfaces, as otherwise its integrity will diminish as duplications and ambiguous records persist.

All application program listings must be controlled and kept fully up to date at all times.

### *11.6.2 Sensitive system isolation*

**This portion of the policy is for "Internal Use" only. All authorized users are requested to contact shahul@kfu.edu.sa, the head of Quality Management Office, for the copy of this portion.**

### *11.7.1 Mobile computing and communications*

Laptops, portables, palmtops, mobile phones with communicator facility, electronic organizers are included within this policy. The detailed policies shall be covered under Desktop and Laptop Policy, which should include the following issues for addressing control measures to mitigate the risk:

- Disclosure of confidential data to unauthorized persons
- Use of unlicensed software can subject KFU to legal action
- Viruses, worms, Trojans and other malicious code can corrupt both data and the system files.
- Theft
- Inadequate backup and recovery routines can lead to the loss of data

Persons who are issued with such mobile computing facilities and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimize the risks.

### *11.7.2 Tele-working (off-site computer usage)*

Tele-working is where staff work from home, or another nominated location, away from the normal office environment.

All issues and risks as highlighted under section 11.7.1 Mobile computing and communications is also applicable on Tele-working and, therefore, similar control measures need to be taken in this respect.

## 12. Security Controls on Systems Acquisition, Development & Maintenance

### *12.1.1 Security requirements of information systems*

All software, from the operating system to applications, need to be updated periodically. Whether this is a simple upgrade or a complete re-write of the main application system, it involves a series of steps, depending on the size and complexity of the system.

Considering security requirements of a system as an afterthought may expose the KFU to loss or fraud. Therefore, the information security management (ISM) should ensure that all business requirements for new information systems or enhancements to existing information systems shall specify the requirements for security controls.

The standard RFP (Request for Proposal) template should either cover the security requirement part or refer the security requirement document for compliance when the vendor propose his solution as well as when the scope statement is prepared.

Developing interfacing software systems is a highly technical task and should only be undertaken in a planned and controlled manner by properly qualified personnel.

Whenever there is a need for reformatting of existing data structure in order to meet the interfacing requirement of the newer system or authorized connectivity to external systems, then there is a risk of data modification that should be dealt with in utmost care and must be carried after a proper impact analysis is done.

All application software must be provided with the appropriate level of technical support to ensure that the KFU's business is not compromised by ensuring that any software problems are handled efficiently with their resolution available in an acceptable time.

Power users (super or root users) activities should be monitored and control on users sharing their password with the power user, in the assumption of resolving the problems, need to be restricted. Any such sharing of power user passwords shall be considered as violation of the KFU's policies and may invoke disciplinary action.

### *12.1.2 System Development Life Cycle (SDLC) methodology*

All in-house and outsourced application system development must follow an approved SDLC methodology and this should provide for:

- Standard covering testing requirements, verification, documentation, and retention for the testing of the total system as a part of every information system development or modification project.

- Definition of the circumstances under which parallel or pilot testing of new and/or existing systems will be conducted.
- Detailed procedures/steps/flow diagrams for unit testing, application testing, integration testing, system testing, and load and stress testing, which must be performed according to the project test plan and established testing standards before it is approved by the user.
- All parties involved in testing must be advised and instructed appropriately in order to prevent disclosure of sensitive information used during testing.

### *12.2 Correct processing in applications*

Application processing controls that would be built-in into the programming logic should prevent errors, loss, unauthorized modifications or misuse of information in applications.

This can be achieved by implementing and maintaining detailed controls as follows:

- Data input to applications shall be validated to ensure that this data is correct and appropriate.
- All input source/forms/vouchers need to be verified and approved by the supervisor of the concerned department.
- Counter checking of the input source with the data entered must be performed by staff other than the user who entered the data. Applications systems should cater this need.
- Where ever it is possible, automated or integrated validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
- Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
- Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

### *12.3.1 Cryptographic controls policy*

Cryptographic is primarily concerned with maintaining the privacy of communications, and modern methods use a number of techniques to achieve this. Encryption is the transformation of data into another usually unrecognizable form. The only means to read the data is to de-crypt the data using a (secret) key, in the form of a secret character string, itself encapsulated within a pre-formatted electronic file.

Where it is applicable due to KFU's present or future need for maintaining encryption of the confidential information, a detailed procedures and guidelines for the use of

cryptographic controls for protection of information shall be developed and implemented.

### *12.3.2 Key management*

Electronic keys are used in the above explained cryptographic process, i.e. to encrypt and de-crypt messages, data, and information files, exchanged between parties or stored in systems.

The management of electronic keys to control both the encryption and decryption of sensitive information must always be performed under dual control, with duties being rotated between staff.

## *12.4 Security of system files*

### *12.4.1 Operational software*

All critical systems must be operated and administered using documented procedures in a manner which is both efficient and also effective in protecting the organization's information security.

Clearly documented and tested robust and appropriately scheduled routines must exist for all business critical applications, as per the business requirement.

All problems, including periodic problems need to be registered through the incident management system and root-cause-analysis be performed including recommendation for permanent solution.

Operational shortcuts should be prohibited

Only designated staff may be allowed to have access to operational program libraries.

Formal change control procedures with comprehensive audit trails are to be used to control versions of old programs.

### *12.4.2 Protection of system test data*

All test data must be selected carefully. Ideally, all testing would utilize only realistic test data, expressly created for the purpose. However, in practice that may not be feasible at times, and in such cases if the copy of the current data files are used, then it is imperative that any such temporary test data be treated as live at all times.

This is particularly important because test staff tend to have more system privileges compared to a production environment.

Therefore, the use of live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place.

The test data when they extracted from the production environment should be restricted and detailed approval procedure/guidelines must be established and practiced for any such cases that would require the use of production data. This procedure/guideline must address the cleaning of such production data from the test environment in safe manner.

### *12.4.3 Access control to program source code*

Managing the program source code libraries, including objects and all compiling procedures, is very critical for maintaining the information and information processing security. The following rules should be strictly adhered:

- Live (production) and Development libraries must always be kept separate
- Program source code control and maintenance of the source libraries are the responsibility of the IT application development and support department.
- Head of IT application development department or his delegated responsibility must ensure that access to program source libraries are provided only to designated staff.
- IT application development department is responsible for ensuring Who is responsible to ensure they are available and for maintaining them, providing access, escalations if source code is not available etc.
- Only designated staff may access program source libraries.
- Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control.
- Program listings must be controlled and kept fully up to date at all times.
- Periodical checking of the availability of current version of source codes must be performed (at least quarterly once) and escalations if source code is not available need to be addressed to ISM and the Dean of IT, along with the comments on the impact of the unavailability of the source code. Any such kind of issues relating to business critical applications must be escalated to the business owners and to the Information Security Governance Committee.

## *12.5 Security in development and support processes*

Security of application system software and information is very important to support the growth requirement as well as the business continuity of the organization.

### 12.5.1 Change control procedures:

The change management policies and procedures as specified in section 10.1.2. must be applied strictly.

### 12.5.2 Technical Review of applications after operating system changes:

Necessary upgrades to the operating system of any of the KFU's information systems must have the associated risks identified and be carefully planned, incorporating tested fall-back procedures. All such upgrade being undertaken as a formal project.

All business critical applications relying on the changed operating system(s) should be tested to ensure there is no adverse impact on information security.

Operating systems must be regularly monitored and all required housekeeping routines adhered to.

### 12.5.3 Restrictions on changes to software packages:

Modifications to software packages must be routed through change management process (refer to section 10.1.2), and frequent changes should be discouraged.

### 12.5.4 Information leakage:

Opportunities for information leakage should be prevented.

### 12.5.5 Outsourced software development:

All information security related policies, procedures and guidelines applicable on third-party service agreements would be automatically applied in outsourced software development.

All outsourced software development must be supervised and monitored by the internal staff of information technology development department.

### *12.6 Technical vulnerability management*

Asset owners/custodians should be made accountable and responsible to assess the vulnerabilities, corresponding threats and implementing mitigation controls.

Timely information about technical vulnerabilities of information systems being used shall be obtained, the KFU's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

## 13. Information Security Incident Management Policy

All information security incidents have to be evaluated according to their particular circumstances, and this may, or may not, requires various organizational units within the KFU (deanships and/or departments) to be involved: Management, Technical, Human Resources, Legal and the owners of information systems or data.

If it appears that disciplinary action against a member of staff is required, this must be handled with tact and in coordination with HR administration department.(Please refer to section 8.2.3 of this policy manual).

A detailed set of procedures and guidelines must be developed, implemented and maintained in order to ensure information security events weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. Such procedure should consider the following:

- Reporting information security events shall be through appropriate management channels as quickly as possible. 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

## 14. Business Continuity Management (BCM) Policy

In order to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption; a proper planning, designing and developing and testing the plan should be considered with business owner's involvement.

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:

- A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organizations business continuity.
- Each deanship and departments of the KFU should ensure that BCM exists for them. All BCM plans for business continuity of their respective area of concern should be tested at least annually once, taking all the significant changes to the business into account.
- All events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security. 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.
- Detailed plans and procedures should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of critical business processes.
- A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements and to identify priorities for testing and maintenance.
- 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.
- A designated person shall be nominated as the BCM (Business Continuity Manager) and this must be done by a committee such as Information Security Governance Committee or the president of the KFU.
- A designated person shall be nominated as the owner of DR (Disaster Recovery) plan and processes and this must be done by the Dean of IT. The DR plan shall address all the IT related business continuity part of the BCP and, therefore, shall be effectively coordinated by the DR responsible or by another coordinator who will ensure the business involvement of the DR plan and testing process.

- There should exist a proper plan and approved schedule for routine testing of the business continuity plans (BCP) in order to ensure that the plan is up to date and effective.
- The change management process should always make an update and checking on the business continuity plan and improving the back-up site accordingly.
- At least annually once the plan should be reviewed by all the stakeholders and it should be approved by the Information Security Governance Committee.

## 15. Compliance Policy

### *15.1 Compliance with Legal Requirements*

Compliance with legal requirements is mandatory in order to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

The following controls and guidelines need to be considered for making detailed procedures for immediate implementation:

- All applicable legislation need to be identified and explicitly defined, documented and kept up to date for each information system and the organization.
- Appropriate procedure shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
- Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements.
- Data protection and privacy of personal information should be ensured
- Adequate level of preventive control measures should be implemented to deter users from using information processing facilities for unauthorized purposes.
- Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.
- Students and Faculty contact information is to be classified as highly confidential and secured accordingly.

### *15.2 Compliance with security policies and standards, and technical compliance*

Compliance with security policies and standards, and technical compliance is mandatory in order to ensure compliance of systems with organizational security policies, including this policy, and standards.

The following controls and guidelines need to be considered for making detailed procedures for immediate implementation:

- All deans and department and section managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
- Information systems shall be regularly checked for compliance with security implementation standards.

Any gap to the controls implementation due to technical constraint must be notified to all applicable business owners and the copy of such communication to be sent to the Dean of IT for further escalation or decision making including seeking for providing for investment required or accepting the residual risk thereto.

### *15.3 Information systems audit considerations*

**This portion of the policy is for "Internal Use" only. All authorized users are requested to contact shahul@kfu.edu.sa, the head of Quality Management Office, for the copy of this portion.**

## 16. Disciplinary Action and KFU Rights

Failure to adhere to this policy may result in the employee being asked to give a written explanation or other disciplinary action may be taken according to the Human Resources Administration Department policies. Such disciplinary actions shall include, but not limited to:

### *a. Users responsibility for compliance with regulatory and KFU information security policy obligations*

KFU employees, faculty, contracted resources and the students who have been allowed to use the KFU information technology resources, have the obligation and responsibility to be aware of the regulatory obligations on information security relevant to their job duties.

### *b. Protecting Evidence from Destruction*

Special care must be given in maintaining data that may be evidence for unauthorized actions.

### *c. Disciplinary Action and Legal Issues*

Disciplinary action range from a verbal warning to suspension, employment contract termination, or even to criminal prosecution (or other legal action). The HR policy of the KFU shall be referred for this purpose. The following activities may result in disciplinary actions:

**Intellectual Property Rights:**

All works (applications, software, source code, documentation, manuals, project deliverables etc.) produced on behalf of the KFU either by KFU employees or third parties are the property of the KFU.

KFU has the intellectual property rights for the work performed by employees when they are tele-working.

**Deactivation of User Accounts / User Names:**

User accounts will be deactivated / locked after a period of inactivity. When user resumes his duties the account will be activated anew by the Department Manager, after relevant request has been issued.

**Internet and E-mail Access Revocation:**

The KFU reserves the right to revoke access to the Internet and e-mail in case of inappropriate use. The KFU holds the right to define what is considered inappropriate.

**Collection of Usage Statistics:**

Users must be aware that the KFU, following well - accepted practices and the law, may collect statistical data regarding the usage of the e-mail systems and the Internet, in order to allow the technical personnel to ensure the systems' operation, availability, reliability and maintenance.

**Communications Monitoring:**

Employees must be aware that the KFU may inspect samples of communications that take place using its systems, in accordance with the law. KFU does not monitor the content of employee communications (e.g. E-mail messages, Internet access) but reserves the right to conduct legitimate, clearly scoped, defined sample monitoring, in accordance with the law.

**Enforcement::**

Any employee or contractor or student or faculty found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract or admission.

## Annexure

To be added on the folder as attachment.