INFORMATION SECURITY POLICIES

Supplementary Document of Kuwait University Information Security Policy Statements.
Audience
The intended audience for this document includes the following categories of individuals:

- System managers, executives, and information officers making decisions about initiatives.
- Security professionals, including security officers, security administrators, auditors, and others with responsibility for information technology security.
- Information technology program managers.
- System and network administrators.
- Users of public computing services.

Privacy Policy Statement
This privacy policy has been compiled to better serve those who are concerned with how their 'Personally identifiable information' (PII) is being used online. PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Please read our privacy policy carefully to get a clear understanding of how we collect, use, protect or otherwise handle your Personally Identifiable Information in accordance with our website.

What personal information do we collect from the people that visit our blog, website or app?
When registering on our site, as appropriate, you may be asked to enter your name, email address, mailing address, phone number or other details to help you with your experience.

When do we collect information?
We collect information from you when you register on our site, fill out a form or enter information on our site.

How do we use your information?
We may use the information we collect from you when you register sign up for our newsletter, respond to a survey, surf the website, or use certain other site features in the following ways:

- To personalize user's experience and to allow us to deliver the type of content and product offerings in which you are most interested.
- To improve our website in order to better serve you

How do we protect visitor information?
Our website is scanned on a regular basis for security holes and known vulnerabilities in order to make your visit to our site as safe as possible.

Your personal information is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems, and are required to keep the information confidential. In addition, all sensitive/credit information you supply is encrypted via Secure Socket Layer (SSL) technology.

We implement a variety of security measures when a user enters, submits, or accesses their information to maintain the safety of your personal information.

All transactions are processed through a gateway provider and are not stored or processed on our servers.

Do we use 'cookies'?

Yes. Cookies are small files that a site or its service provider transfers to your computer's hard drive through your Web browser (if you allow) that enables the site's or service provider's systems to recognize your browser and capture and remember certain information. They are used to help us understand your preferences based on previous or current site activity, which enables us to provide you with improved services. We also use cookies to help us compile aggregate data about site traffic and site interaction so that we can offer better site experiences and tools in the future. We use cookies to:

- Understand and save user's preferences for future visits.
- Compile aggregate data about site traffic and site interactions in order to offer better site experiences and tools in the future. We may also use trusted third party services that track this information on our behalf.

You can choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off all cookies. You do this through your browser (like Internet Explorer) settings. Each browser is a little different, so look at your browser's Help menu to learn the correct way to modify your cookies.

If you disable cookies off, some features will be disabled. It will affect the users experience that make your site experience more efficient and some of our services will not function properly.

Third Party Disclosure

We do not sell, trade, or otherwise transfer to outside parties your personally identifiable information unless we provide you with advance notice. This does not include website hosting partners and other parties who assist us in
operating our website, conducting our business, or servicing you, so long as those parties agree to keep this information confidential. We may also release your information when we believe release is appropriate to comply with the law, enforce our site policies, or protect ours or others’ rights, property, or safety.

Third party links

Occasionally, at our discretion, we may include or offer third party services on our website. These third party sites have separate and independent privacy policies. We therefore have no responsibility or liability for the content and activities of these linked sites. Nonetheless, we seek to protect the integrity of our site and welcome any feedback about these sites.

Google

We have not enabled Google AdSense on our site but we may do so in the future.

Fair Information Practices

The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information.

In order to be in line with Fair Information Practices we will take the following responsive action, should a data breach occur:

We will notify the users via in site notification within an appropriate period, whilst we undergo the suitable security measurements.

We also agree to the individual redress principle, which requires that individuals have a right to pursue legally enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or a government agency to investigate and/or prosecute non-compliance by data processors.

If there are any questions regarding this privacy policy you may contact us using the information below.

Email: itsecurity@ku.edu.kw
Security Policies:

1. Information Systems Terms of Use

1.1 Purpose

KUWAIT UNIVERSITY considers its information resources (i.e. information maintained in electronic form and systems that process, store or transmit such information) as assets.

This policy documents the responsibilities of the users of Kuwait University’s information resources. Compliance with this policy is essential in creating an environment that is conducive to sound security practices.

1.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information.

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact their line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.
1.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security.
- Custodians responsible for implementing this policy are listed in Section 1.9.

1.4 Definitions

Definition of some of the common terms:

- **Critical**: Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.
- **Information Asset**: Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.
- **Sensitive**: Concerned with highly classified information or involving discretionary authority over important official matters.

1.5 Basic Assumptions

(None)

1.6 Policy Statements

Please read these Terms of Use ("Terms") carefully before accessing or participating in any chat room, newsgroup, bulletin board, mailing list, website, transaction or other on-line forum available at kuniv.edu or other Kuwait University sites. By using and participating in these sites, you signify that you have read these terms and agree to be bound by and comply with them. If you do not agree to be bound by these terms, please promptly exit all sites. Kuwait University reserves the right to modify these terms at any time and will publish notice of any such modifications on-line at this site or elsewhere on-line. By continuing to access a site after notice of such modifications has been published, you signify your agreement to be bound by them.

1.6.1 Disclaimer

Sites may include immoderate forums containing the personal opinions and other expressions of the people who post entries on a wide range of topics. Neither the content of these Sites, nor the links to other web sites, are screened, approved, reviewed or endorsed by Kuwait University. The text and
other material on these Sites are the opinion of the specific author and are not statements of advice, opinion, or information of Kuwait University. If you feel you might be offended by the content of the Sites, you should not continue.

1.6.2 Rules for Online Conduct

You agree to use the Sites in accordance with all applicable laws. Because Kuwait University is a non-profit organization, you agree that you will not use the Site for organized partisan political activities. You further agree that you will not e-mail or post any of the following content anywhere on the Site, or on any other Kuwait University computing resources:

- Content that defames or threatens others
- Harassing statements or content that violates federal or state law
- Content that discusses illegal activities with the intent to commit them
- Content that infringes another's intellectual property, including, but not limited to, copyrights, trademarks or trade secrets
- Material that contains obscene (i.e. pornographic) language or images
- Advertising or any form of commercial solicitation
- Content that is otherwise illegal

Copyrighted material, including without limitation software, graphics, text, photographs, sound, video and musical recordings, may not be placed on the Site without the express permission of the owner of the copyright in the material, or other legal entitlement to use the material.

Kuwait University students using this Site are expected to abide by the Fundamental Standard which has set the standard of conduct for students at Kuwait University since 1966 and which provides:

"Subject.7: Students in relation to the university should respect university standard systems; furthermore he shall build his relations with the university family upon kindness and respect to others rights."

"Subject.8: It is strictly prohibited to insult University members; should they be students, employees, or faculty; may that be on a personal level or referring to their dignity"

Although Kuwait University does not routinely, screen or monitor content posted by users to the Site, Kuwait University reserves the right to remove content, which violates the above rules of which it becomes aware, but is under no obligation to do so. Finally, you agree that you will not access or attempt to
access any other user’s account, or misrepresent or attempt to misrepresent your identity while using the Sites.

1.6.3 Permission to Use Materials

In consideration for your agreement to the terms and conditions contained here, Kuwait University grants you a personal, non-exclusive, non-transferable license to access and use the Sites. User may download material from the Sites only for User's own personal, non-commercial use. User may not otherwise copy, reproduce, retransmit, distribute, publish, commercially exploit or otherwise transfer any material. The burden of determining that use of any information, software or any other content on the Site is permissible rests with User.

1.6.4 Limitation of Use

You may use sites for legal purposes only. Furthermore, you agree that, if a third party claims that any material you have contributed to a site is unlawful, you will bear the burden of establishing that the material complies with all applicable laws. Although Kuwait University does not monitor the content of the sites, Kuwait University has the right to remove material from the sites, block access, or take other action with respect to the Material in its sole discretion, although Kuwait University is under no obligation to do so. You may not use Kuwait University computing resources or sites to disseminate unsolicited advertising or promotional material of any kind.

1.6.5 Links to Other Sites

Kuwait University’s Site may include hyperlinks to websites maintained or controlled by others. Kuwait University is not responsible for and does not routinely screen, approve, review or endorse the contents of or use of any of the products or services that may be offered at these websites.

1.6.6 Choice of Law/Forum Selection

Sites are hosted by Kuwait University on computing resources located on Kuwait University campus or elsewhere. You agree that any dispute arising out of or relating to these Terms or any content posted to a Site, including copies and republication thereof, whether based in contract, tort, statutory or other law, will be governed by the laws of the State of Kuwait.
1.6.7 Disclaimer of Warranty/Limitation of Liability

THESE SITES AND ANY INFORMATION, PRODUCTS OR SERVICES THEREIN ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR USE OF A PARTICULAR PURPOSE, OR NONINFRINGEMENT.

Kuwait University does not warrant, and hereby disclaims any warranties, either express or implied, with respect to the accuracy, adequacy or completeness of any Site, information obtained from a Site, or link to a Site. Kuwait University does not warrant that Sites will operate in an uninterrupted or error-free manner or that Sites are free of viruses or other harmful components. Use of information obtained from or through these Sites is at your own risk.

YOU AGREE THAT KUWAIT UNIVERSITY WILL NOT BE LIABLE TO YOU FOR ANY LOSS OR DAMAGES, EITHER ACTUAL OR CONSEQUENTIAL, ARISING OUT OF OR RELATING TO THESE TERMS, OR TO YOUR (OR ANY THIRD PARTY’S) USE OR INABILITY TO USE A SITE, OR TO YOUR PLACEMENT OF CONTENT ON A SITE, OR TO YOUR RELIANCE UPON INFORMATION OBTAINED FROM OR THROUGH A SITE. IN PARTICULAR, KUWAIT UNIVERSITY WILL HAVE NO LIABILITY FOR ANY CONSEQUENTIAL, INDIRECT, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE, (INCLUDING, BUT NOT LIMITED TO, CLAIMS FOR ERRORS, LOSS OF DATA, OR INTERRUPTION IN AVAILABILITY OF DATA), ARISING OUT OF OR RELATING TO THESE TERMS, YOUR USE OR INABILITY TO USE A SITE, OR ANY PURCHASES ON THIS SITE, OR YOUR PLACEMENT OF CONTENT ON A SITE, OR TO YOUR RELIANCE UPON INFORMATION OBTAINED FROM OR THROUGH A SITE, WHETHER BASED IN CONTRACT, TORT, STATUTORY OR OTHER LAW, EXCEPT ONLY IN THE CASE OF DEATH OR PERSONAL INJURY WHERE AND ONLY TO THE EXTENT THAT APPLICABLE LAW REQUIRES SUCH LIABILITY.

Kuwait University makes no representation regarding your ability to transmit and receive information from or through the Sites and you agree and acknowledge that your ability to access the Sites may be impaired. Kuwait University disclaims any liability resulting from or related to such events.

1.6.8 Trademarks

The logo, name and all graphics on the Sites of Kuwait University, or any of its affiliates, are trademarks of Kuwait University or its affiliates. Use, reproduction, copying or redistribution of trademarks, without the written permission of Kuwait University or its affiliates is prohibited. All other trademarks or service marks appearing on the Site are the marks of their respective owners.
1.6.9 Indemnification

You agree to indemnify and hold Kuwait University harmless from any claims, losses or damages, including legal fees, resulting from your violation of these Terms, your use of a Site or your placement of any content onto a Site, and to fully cooperate in Kuwait University’s defense against any such claims.

1.6.10 Your Account

If you use this site, you are responsible for maintaining the confidentiality of your account and password, if any, and for restricting access to your computer, and you agree to accept responsibility for all activities that occur under your account or password.

1.6.11 Other

The Sites may contain errors and omissions relating to product description, pricing and availability. We reserve the right to correct errors or omissions without prior notice. We also reserve the right to cancel any offered product or service in the event of an error or omission in the description, including price, unavailability or other reason.

1.6.12 General

These Terms constitute the entire agreement between you and Kuwait University and its affiliates with respect to the subject matter herein and supersedes any prior or contemporaneous oral or written agreements.

1.6.13 Acceptable Usage

1.6.13.1 Usage of KUWAIT UNIVERSITY Information Systems

1.6.13.1.1 Users are only authorized to utilize KUWAIT UNIVERSITY information resources for academic purposes for which they have been authorized. Usage of KUWAIT UNIVERSITY information systems and resources for personal usage or on behalf of third party (i.e., personal client, family member, political or religious or charitable or school/organization, etc.) is strictly prohibited.
1.6.13.2 Unauthorized Copies of Licensed Software & Hardware

1.6.13.2.1 Introduction of unauthorized copies of licensed software and hardware (piracy/copyright & patent infringement) to KUWAIT UNIVERSITY information resources and the copying of such material is prohibited

1.6.13.2.2 The storage, processing, or transmittal of unauthorized copies of licensed software and hardware (piracy/copyright & patent infringement) by KUWAIT UNIVERSITY personnel associates is strictly prohibited

1.6.13.3 Freeware and Shareware Applications

1.6.13.3.1 Introduction of freeware and shareware software whether downloaded from internet or obtained through any other media to KUWAIT UNIVERSITY information systems will be subject to a formal evaluation and approval process

1.6.13.3.2 Freeware and shareware applications must be evaluated and tested before installation on KUWAIT UNIVERSITY information resources is permitted

1.6.13.4 Usage of KUWAIT UNIVERSITY Information Resources to Store, Process, Download, or Transmit Data

1.6.13.4.1 Downloading, redistribution and printing of copyrighted articles, documents, or other copyrighted materials to KUWAIT UNIVERSITY information systems are strictly prohibited

1.6.13.4.2 Receiving, printing, transmitting, or otherwise disseminating proprietary data, company secrets, or other confidential information in violation of company policy or proprietary agreements is strictly prohibited

1.6.13.4.3 Downloading inappropriate material such as picture files, music files, or video files or games for personal use is strictly prohibited

1.6.13.4.4 Employees should not use company's Information systems for viewing, transmitting, receiving or storage of any non-business material that may be
seen by other persons as insulting, disruptive, offensive, culturally sensitive, or harmful to morale.

1.6.13.4.5 Examples of forbidden transmissions include messages and/or images that are sexually-explicit, offensive, ethnic or racial slurs, and/or any other material that can be construed to be harassment or degradation of others based on their sex, race, age, national origin, religion or political beliefs.

1.6.13.5 Due Diligence

1.6.13.5.1 Each user has the responsibility to notify line manager, IS Helpdesk, system administrator, department head who in turn will report to the Manager Information Security immediately of any evidence or suspicion of any security violation with regard to:

- Unauthorized access to network, telecommunications, or computer systems;
- The apparent presence of a virus on a PC;
- The apparent presence of any information resource prohibited by this policy;
- Apparent tampering with any file for which the user established restrictive discretionary access controls; and
- Violation of this policy or any other Information security policy or procedure by another user, employee, contractor or third party service provider.

1.6.13.5.2 Each user has the responsibility to prevent unauthorized access including viewing, of information resources in his possession or control (such as portable computer or desktop terminal/computer or printouts or floppy/tape media).

1.6.13.5.3 Each user is responsible for safeguarding his access security privileges against unauthorized access by colleagues, customers/clients, vendors, relatives, friends, and unknown visitors. In situations where such people must be provided access (e.g., a vendor who has come to install a product or make repairs), then the user must oversee and monitor the actions of the individual given temporary access.
1.6.13.6  Destructive Programs and Games

1.6.13.6.1  Destructive programs (e.g., viruses, self-replicating code) that cause damage, interfere with other programs, gain unauthorized access, or impact Kuwait University’s information systems is strictly prohibited

1.6.13.6.2  Games are not permitted and must be removed from all systems.

1.6.13.7  External Services

1.6.13.7.1  All users must limit their usage of external services (e.g., bulletin board, on-line service provider, Internet site, commercial database) to authorized business purposes only in accordance with this policy, standards, and procedures regarding such usage and as approved by the user’s management

1.6.13.7.2  Any exploration of the public internet domain for business related research is acceptable provided the user complies with KUWAIT UNIVERSITY policies, standards, and procedures regarding such usage and they comply with the policies, standards, and procedures of the explored site

1.6.13.8  Electronic Mail and Posting to Bulletin Boards, Mailing Lists, & news Groups

1.6.13.8.1  Refer to Internet & E-Mail security policy for guidelines on electronic mail and postings to bulletin boards, mailing lists and news groups

1.7  Related Information Security Policies

- Corporate Security Policy
- Internet & E-Mail Security Policy
- Virus & Malware Protection Policy
- Password Policy
- Access Control Policy

1.8  Compliance Measurement

Compliance with Information Systems Terms of Use is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.
• Compliance with Information Systems Acceptable use Policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
• Compliance measurement should also include periodic review for Security Quality Assurance.
• Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  ❖ Verbal or written warning
  ❖ Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

### 1.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>All Users / Managers</td>
<td>Security / IT</td>
</tr>
<tr>
<td>6.2</td>
<td>All Users / Managers</td>
<td>Information</td>
</tr>
</tbody>
</table>

### 2 Internet & E-Mail Security Policy

#### 2.1 Purpose

The purpose of the policy is to minimize risk associated with Internet and
services, and defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

2.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.

2.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security
- Custodians responsible for implementing this policy are listed in Section 9

2.4 Definitions

Definition of some of the common terms:

**Critical:** Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.
**Information Asset:** Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.

**Sensitive:** Concerned with highly classified information or involving discretionary authority over important official matters.

2.5 **Basic Assumptions**

(None)

2.6 **Policy Statements**

2.6.1 **Internet Security Policies**

2.6.1.1 **Reliance of Information downloaded from the Internet**

2.6.1.1.1 *Information taken from the Internet should not be relied on until confirmed by separate information from another source.*

There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Unless tools and solutions like Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP), and Public Key Infrastructures (PKI - certificate authority based solutions) are used, it is also relatively easy to spoof another user on the Internet.

2.6.1.2 **Release of KUWAIT UNIVERSITY Information on the Internet**

2.6.1.2.1 *Users should not release any KUWAIT UNIVERSITY information over the Internet. Further, users should not place KUWAIT UNIVERSITY material (software, internal memos, etc.) on any publicly accessible Internet computer.*

2.6.1.2.2 *Web page content should be in accordance with specific company directives, and the page layout must follow the policies/guidelines defined by Manager Information Security*
2.6.2 Information Protection

2.6.2.1 KUWAIT UNIVERSITY’s sensitive and confidential information should never be sent over the Internet unless it has first been encrypted by approved methods.

2.6.2.2 Unless specifically known to be in the public domain, source code should always be encrypted before being sent over the Internet.

2.6.2.3 Credit card numbers, telephone calling card numbers, login passwords, and other parameters that can be used to gain access to goods or services, should not be sent over the Internet in readable form. An encryption algorithm approved by Manager Information Security should be used to protect these parameters as they traverse the Internet.

2.6.2.4 Reporting Security Problems

2.6.2.4.1 Each user has the responsibility to notify the Line manager, IS Helpdesk, who in turn will notify the Manager Information Security immediately of any evidence of any security violation involving Internet connectivity in regard to:

- Unauthorized access to network, telecommunications, or computer systems;
- Apparent transmittal of a virus or worm via networking technologies; and
- Apparent tampering with any file for which the user established restrictive discretionary access controls.

2.6.2.5 Expectation of Privacy

2.6.2.5.1 Users of KUWAIT UNIVERSITY’s information assets and/or the Internet should not send private information over the Internet, unless encrypted.

2.6.2.6 Resource Utilization

2.6.2.6.1 Use of Internet services shall be limited to company-related activities; users must not utilize the company’s network resources for other purposes rather than company related activities.
2.6.2.7 Public Representations

2.6.2.7.1 KUWAIT UNIVERSITY employees, personnel, or third party contractors using KUWAIT UNIVERSITY facilities should not indicate their affiliation with KUWAIT UNIVERSITY in bulletin board discussions, chat sessions, and other offerings on the Internet.

2.6.2.7.2 KUWAIT UNIVERSITY employees, personnel, or third party contractors using KUWAIT UNIVERSITY facilities should not publicly disclose internal KUWAIT UNIVERSITY information via the Internet that may adversely affect KUWAIT UNIVERSITY, KUWAIT UNIVERSITY’s customer relations, or public image.

2.6.2.7.3 Users should not post network or server configuration information about any KUWAIT UNIVERSITY information systems to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.

2.6.2.7.4 Users should ensure that postings on to mailing lists, public news groups and related websites do not reveal details of KUWAIT UNIVERSITY’s internal functioning, infrastructure or potential vulnerabilities in KUWAIT UNIVERSITY’s Information Security infrastructure.

2.6.2.7.5 Only authorized KUWAIT UNIVERSITY personnel or third party contractors may establish Internet or other external network connections. These connections include the establishment of multi-computer file systems.

2.6.2.8 Configuration Management

2.6.2.8.1 All configuration details (All hardware devices/components, all operating system and application software, all firmware components, physical and logical network addresses, and connecting circuit numbers) of Internet connectivity network architecture must be completely documented and maintained.
2.6.2.9 Periodic Review of Authorized Accounts

2.6.2.9.1 The administrator should periodically reconfirm the validity of all log-ins and electronic mail authorizations. The period between reconfirmation should not exceed six months.

2.6.3 Internet Usage

2.6.3.1 Password Access Requirements

2.6.3.1.1 The password should meet KUWAIT UNIVERSITY password requirements as described in the password policy. The user should comply with the most restrictive of the passwords format specified

2.6.3.2 User Authorization and Verification

2.6.3.2.1 Each user having login access to the internet connection should have a unique User ID

2.6.3.3 Requesting and Granting User Authorization

2.6.3.3.1 Each personnel requesting a user ID should provide an authorization from the head of his business unit

2.6.3.3.2 Requests for an Internet connection should be accompanied by a justification for such access. The request must be authorized by the Users Manager

2.6.3.3.3 An associate that requires only the inclusion of an electronic mail alias entry should establish authorization in the same manner as that described for a login user.

2.6.3.4 Viruses and Malicious Software Protection

2.6.3.4.1 Users are not allowed to run programs obtained from external sources (via the WWW or other non-trusted source) without prior permission from the Administrator of Information Security and virus protection checks.
2.6.3.4.2 Users should never download files directly into a network server or production machine. Downloads should be directed to a separated (isolated) environment or removable storage media. Upon successful completion of the procedures described on the previous paragraph, users shall move the downloaded files to their working directories. Moves to production machine (or equivalent) can only be performed with documented approval from System Owner.

2.6.3.5 Confidentiality

2.6.3.5.1 No sensitive information should be transmitted over the Internet and the World-Wide Web (for example through Web based E-Mail systems) without first being encrypted.

2.6.4 Internet Networking Services

2.6.4.1 File Transfer Protocol (FTP)

2.6.4.1.1 Only users that have a job or business need to use FTP shall be authorized to use SFTP

2.6.4.1.2 No inbound FTP shall be allowed under any circumstances from the internet to the firewall or the internal LAN

2.6.4.1.3 Outbound FTP shall be allowed only via proxy accounts on the firewall system

2.6.4.1.4 Users shall not use FTP services to any remote host machine on which they do not have accounts. This does not apply to sites that offer or advertise an anonymous FTP service

2.6.4.1.5 All files that are downloaded via FTP should undergo a virus check on a system, which is not directly connected to the internet or the internal network

2.6.4.1.6 It is preferred to use SFTP at all times
2.6.4.2 Telnet Services

2.6.4.2.1 No inbound Telnet access from the internet should be allowed

2.6.4.2.2 All outbound Telnet access shall be from a proxy account on the firewall

2.6.4.2.3 All authorized Telnet connection should be logged

2.6.4.2.4 Users shall not Telnet into ports other than the standard Telnet port. Telnets into ports designated for mail, FTP or WWW or other internet services are strictly forbidden.

2.6.4.2.5 It is always preferred to use SSH where ever possible

2.6.4.3 Network News

2.6.4.3.1 Inbound News feeds should be subscription to only selected newsgroups for selected User IDs

2.6.4.3.2 No posting to News groups shall be allowed from KUWAIT UNIVERSITY network

2.6.5 General E-Mail Policy

2.6.5.1 E-Mail Usage

2.6.5.1.1 The usage of the E-Mail system is subject to the following:

- E-Mail should be used in compliance with the Corporate Security Policy and associated Supplementary Information Security Policies. All access to electronic messages should be limited to properly authorized personnel.
- Personal or non-business use of the Systems is NOT permitted.

2.6.5.1.2 All E-Mails should comply to KUWAIT UNIVERSITY standards regarding decency and appropriate content. Message content restrictions include:

- KUWAIT UNIVERSITY information resources should not be used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others.
• The Systems should not be used to communicate statements, messages, or images consisting of pornographic material, ethnic slurs, racial epithets, or anything that may be construed as harassing, offensive, or insulting to others based on race, religion, national origin, color, marital status, citizenship status, age, disability, or physical appearance.

• Any statements or comments made via E-Mail that could in any way be considered as an action of KUWAIT UNIVERSITY should bear a disclaimer such as “These statements are solely my own opinion, and do not necessarily reflect the views of my employer.” Even with this disclaimer, all practices regarding decency and appropriate conduct still apply.

2.6.5.1.3 Any use of E-Mail from the network is easily traceable to KUWAIT UNIVERSITY. Personnel should conduct these activities with the reputation of KUWAIT UNIVERSITY in mind. Staff should exercise the same care in drafting E-Mail, as they would for any other written communication that bears KUWAIT UNIVERSITY name.

2.6.5.1.4 KUWAIT UNIVERSITY E-Mail systems should not be used to produce or distribute “chain mail,” operates a business, or makes solicitations for personal gain, political or religious causes, or outside organizations. Users should not forward or otherwise propagate, to individuals or groups, chain letters, pyramid schemes or any other types of data that may unnecessarily consume system resources or otherwise interfere with the work of others.

2.6.5.1.5 To maintain the security of KUWAIT UNIVERSITY’s E-Mail system, it is important to control access to the system. Users should not provide other unauthorized persons with their E-Mail ID and personal password.

2.6.5.1.6 Users must use only their own KUWAIT UNIVERSITY official E-Mail account and should not allow anyone else access to their account. Impersonation is not permitted. Users should identify themselves by their real name; pseudonyms that are not readily attributable to actual users should not be allowed. Users should not represent themselves as another user. Each user should take precautions to prevent unauthorized use of the E-Mail account. Forging of header information in E-Mail (including source address, destination address, and timestamps) is not permitted.
2.6.5.1.7 Users should not publish or distribute internal mailing lists to non-staff members.

2.6.5.1.8 KUWAIT UNIVERSITY Systems should not be used to transmit or receive trade secrets, copyrighted materials, or proprietary or confidential information unless it is digitally signed and encrypted.

2.6.5.1.9 Any information regarded as confidential including legal or contractual agreements, technical information related to KUWAIT UNIVERSITY’s operations or security etc. should not be communicated through E-Mail unless it is digitally signed and encrypted.

2.6.5.1.10 Users should not post network or server configuration information about any KUWAIT UNIVERSITY machines to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, software version numbers, etc.

2.6.5.1.11 Information received through unsecured E-Mail is not to be considered private or secure. Clear text information in transit may be vulnerable to interception. Secure communication through E-Mail can be ensured only by using encryption and digital signatures.

2.6.5.1.12 Attachments, links, or mail messages as whole from unknown or untrusted sources should not be opened. All E-Mail attachments, regardless of the source or content, should be scanned for viruses and other destructive programs before being opened or stored on any KUWAIT UNIVERSITY computer system. Personnel should perform a virus scan on all material that is transmitted to other users via E-Mail prior to sending it.

2.6.5.1.13 Users should not send unsolicited bulk mail messages (also known as “junk mail” or “spam”). This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious E-Mail, including but not limited to “mail bombing,” is prohibited.

2.6.5.1.14 Users should not execute or install any programs, upgrades or patches that are received via E-Mail or download from the Internet.
2.6.5.1.15 The Systems and all information contained in the systems (including computer files, E-Mail and voice mail messages, Internet access logs, etc.) are KUWAIT UNIVERSITY’s property. At any time, with or without notice, this information may be monitored, searched, reviewed, disclosed, or intercepted by KUWAIT UNIVERSITY for any legitimate purpose, including the following:

- To monitor performance,
- Ensure compliance with KUWAIT UNIVERSITY policies,
- Prevent misuse of the Systems,
- Troubleshoot hardware and software problems,
- Comply with legal and regulatory requests for information, and
- Investigate disclosure of confidential business, proprietary information, or conduct that may be illegal or adversely affect KUWAIT UNIVERSITY or its associates.

KUWAIT UNIVERSITY may also gain access to communications deleted from the Systems.

2.6.5.1.16 All distributed lists Emails should not include an active link to an Internet website unless approved by Manager Information Security.

2.6.5.2 E-Mail Security Settings

2.6.5.2.1 KUWAIT UNIVERSITY employees, personnel, or third party contractors using KUWAIT UNIVERSITY facilities should not modify the security parameters within KUWAIT UNIVERSITY E-Mail system. Users making unauthorized changes to the E-Mail security parameters are in violation of this policy.

2.6.5.2.2 KUWAIT UNIVERSITY e-mail users shall maintain their passwords to be private and well kept. Passwords shall be a minimum of 6 alphanumeric characters in addition to special characters. Passwords shall be renewed according to their expiry periods, which is set by KUWAIT UNIVERSITY to be a period of 180 days.

2.6.5.3 E-Mail Retention

2.6.5.3.1 Information (mail messages and attachments) on KUWAIT UNIVERSITY’s E-Mail system should be backed up and should be available for recovery for a period of 30 days.
2.6.5.4 E-Mail Attachments

Description

A feature of E-Mail is the ability to send and receive attachments. However, sending large attachments causes mail servers and gateways to external services (such as the Internet) to run slower and can cause significant delay in the delivery of E-Mail. To prevent the degradation of KUWAIT UNIVERSITY’s E-Mail systems, employees should limit the transmission of large attachments.

2.6.5.4.1 All attachments to mails should be limited and compressed using file compression utilities, before sending them.

2.6.5.4.2 Non-business related E-Mail containing large file attachments, such as graphics and multimedia files, should not be sent via KUWAIT UNIVERSITY’s E-Mail systems.

2.6.6 Firewall Configuration

2.6.6.1 Firewall Policy

2.6.6.1.1 KUWAIT UNIVERSITY’s Firewalls shall be configured in accordance with KUWAIT UNIVERSITY’s Firewall Configuration Standards and Procedures document. The following high-level policies should be complied with during configuration of KUWAIT UNIVERSITY’s Internet firewalls:

- All non-essential networking or system services must be eliminated or removed from the firewall.
- The system logs generated from the firewall must be reviewed on a continuing basis to detect any unauthorized entry attempts.
- All unauthorized access through the firewall must be reported to the security manager and network administrator.
- Proxy accounts must be used on the firewall at all times.
- Networking traffic will be subject to filtering based on current security requirements.
2.6.7 Legal

2.6.7.1 KUWAIT UNIVERSITY should comply to all existing laws of Kuwait regulations regarding electronic commerce and the Internet.

2.6.8 World Wide Web Policy (WWW)

2.6.8.1 E-Mail Attachments

2.6.8.1.1 Responsibility for the security administration of KUWAIT UNIVERSITY’s World-Wide Web presence will be borne by the e-Security. In cases where KUWAIT UNIVERSITY’s World-Wide Web (WWW) presence is hosted by a third party, the host site should adhere to the policies defined in this document as well.

2.6.8.1.2 KUWAIT UNIVERSITY’s WWW resources shall be physically secured and appropriately configured to provide:

- Access level security
- Secure hardening of operating systems
- Load balancing and high availability
- Secure network architecture (Perimeter security, Firewall, IPS, DMZ, etc.)
- Associated application and database security

2.6.8.2 Content

2.6.8.2.1 Web applications and content that is placed on KUWAIT UNIVERSITY Web server or servers must be approved by the designated KUWAIT UNIVERSITY management.

2.6.9 Proprietary Information

2.6.9.1 Copyright Clearance

2.6.9.1.1 No proprietary material obtained via the World-Wide Web shall be used company-wide without the proper copyright clearance.
2.6.9.1.2 Clearance can be obtained from the author or copyright owner. Most programs provide information on copyright issues on their documentation (disclaimers) or installation instructions.

2.7 Related Information Security Policies

- Corporate Security Policy
- Password Policy
- Access Control Policy
- Compliance Policy

2.8 Compliance Measurements

Compliance Internet & email Security policy is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

- Compliance with Internet & email Security policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
- Compliance measurement should also include periodic review for Security Quality Assurance.
- Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  - Verbal or written warning
  - Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

2.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>All Users / Manager Information Security / IT</td>
</tr>
<tr>
<td>6.2</td>
<td>All Users / Manager Information Security / IT</td>
</tr>
<tr>
<td>6.3</td>
<td>All Users / Manager Information Security / IT</td>
</tr>
</tbody>
</table>
3 Virus and Malware Protection Policy

3.1 Purpose

Viruses and Malicious Software (Malware) are a potential risk to the confidentiality, integrity and availability of Kuwait University's Information Systems.

This document relates Kuwait University’s policy for the prevention, detection and removal of Viruses and Malware.

3.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information.
Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.

### 3.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security
- Custodians responsible for implementing this policy are listed in Section 3.9

### 3.4 Definitions

Definition of some of the common terms:

**Critical:** Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

**Information Asset:** Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.

**Sensitive:** Concerned with highly classified information or involving discretionary authority over important official matters.

### 3.5 Basic Assumptions

(None)

### 3.6 Policy Statements

The objective of this policy is to protect the integrity of software and information. Precautions are required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network
worms, Trojan horses and logic bombs. Users should be made aware of the dangers of unauthorized or malicious software, and managers should, where appropriate, introduce special controls to detect or prevent its introduction. In particular, it is essential that precautions be taken to detect and prevent computer viruses on personal computers.

Viruses and Malware are unauthorized programs that may replicate themselves and spread to other computer systems across a network. The symptoms of Virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.

3.6.1 Virus & Malware Protection Policy

3.6.1.1 Prevention of Viruses & Malware from affecting KUWAIT UNIVERSITY Information Systems

3.6.1.1.1 All University members; including students, faculty, or employees who possess machines or systems provided by KUWAIT UNIVERSITY shall be obliged to install the standard Protection client provided by KUWAIT UNIVERSITY. All possible and practicable measure shall be taken to prevent the introduction of Viruses and Malware into Kuwait University’s information systems.

3.6.1.1.2 Gateway virus protection shall be enabled for HTTP, SFTP & SMTP traffic.

3.6.1.1.3 Antivirus / AntiMalware measures would include but are not limited to the following:-

- Virus and Malware detection infrastructure shall be implemented at points where Viruses and Malware can be introduced into Kuwait University’s network.
- Kuwait University’s process to update the Virus and Malware detection infrastructure with the latest product and Virus signature updates as soon as these updates are released must be implemented.
- The installation of Virus and Malware protection software on any new potential point of entry (new PC’s, servers, etc.) of Viruses or Malware or to determine that the new (potential) point of entry is covered by an
existing installation of such software must be in accordance with the defined procedures.

- Kuwait University’s process to ensure that Virus and Malware detection infrastructure remains active and is not disabled at any potential entry point must be implemented.
- Configuration should be such that, the anti-virus updates can be installed automatically on the computers with little or no user intervention
- Educating all users on symptoms and best practices.
- Anti virus must automatically check removable media like CD, USB drives when attached to and KUWAIT UNIVERSITY system / network.

3.6.1.1.4 The integrity of software used on any KUWAIT UNIVERSITY IT resource must be assured by ensuring that software is purchased from a reputable company and tested for malware before installation (e.g. screensavers and demonstration software etc.)

3.6.1.1.5 Strict disciplines should be imposed over the downloading of mobile code from the web, and should include:

- restricting the use of mobile code from undesirable sources, such as by producing a ‘white list’ of code only allowed from specified web sites
- preventing the downloading of specific types of mobile code with known vulnerabilities, such as ActiveX controls
- using cryptographic techniques, such as code signing, to confirm that downloaded mobile code comes from a recognized source and has not been tampered with
- Screening mobile code in quarantine areas, for example, using a ‘sandbox’, prior to use.

3.6.1.2 Detection of Viruses & Malware on KUWAIT UNIVERSITY Information Systems

3.6.1.2.1 All possible and practicable measures must be taken to detect Viruses and Malware on Kuwait University’s information systems infrastructure.

3.6.1.2.2 These measures would include but are not limited to the following:-

- Implementation of memory resident components of Virus and Malware detection infrastructure in PC’s, servers, laptop computers and other appropriate components of Kuwait University’s information systems infrastructure.
- Anti-Virus software scans must be performed on all PC’s, servers, laptop computers and other components of Kuwait University’s information systems architecture at periodic intervals to detect potential Viruses and Malware.
- Kuwait University’s process must be implemented to update the Virus and Malware detection infrastructure with the latest product and Virus signature updates as soon as these updates are released.
- Kuwait University’s process must be implemented to install Virus and Malware protection software on any new components (new PC’s, servers, etc.) of the network or to determine that the new (potential) point of entry is covered by an existing installation of such software.
- The steps /decisions to be taken in the event of the entry of a Virus into Kuwait University’s information systems infrastructure must be in accordance with the Incident response procedures.

3.6.1.3 Removing Viruses & Malware from infected components of the Infrastructure

3.6.1.3.1 All files downloaded from the internet or email systems, or introduced via CD ROMs or through any other media or interconnection / networking facility must be scanned for Viruses and Malware.

3.6.1.3.2 Where Viruses or Malware are identified / detected:

- The infected system must be immediately isolated (through notice or by force; as the security requirements demand) from the network infrastructure and handled in accordance with the Virus and Malware Contingency Plan.
- The Virus must be removed using appropriate anti-Virus software.
- Virus scans of all components of the Information Systems infrastructure must be conducted to detect any further cases of infection.
- The Desktop support team (helpdesk) must investigate the path used by the Virus to enter the network and appropriate prevention measures must be implemented to prevent recurrence.

3.6.1.4 User Responsibilities

3.6.1.4.1 Users must be prohibited from changing the configuration of, removing, de-activation or otherwise tampering with any Virus and Malware prevention / detection and software that has been installed on systems used by them.
3.6.1.4.2 Users must report all incidences of Virus (detected by the installed anti-Virus software) immediately to Manager Information Security. The infected system must be immediately isolated from the network infrastructure and handled in accordance with the Incident Response Procedures.

3.6.1.4.3 It is the responsibility of users to ensure that all anti-Virus updates made available to them are immediately implemented on the workstations, desktops, laptops, other equipment assigned to them.

3.6.1.4.4 Users must ensure that exchanges of media with other organization are checked for viruses and malware.

3.6.1.4.5 Users should always run the corporate standard anti-virus software.

3.6.1.4.6 Users should never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. They should delete these attachments immediately, then "double delete" them by emptying your Trash.

3.6.1.4.7 Users delete spam, chain, and other junk email without forwarding.

3.6.1.4.8 Users should never download files from unknown or suspicious sources.

3.6.1.4.9 Users will avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

3.7 Related Information Security Policies

- Corporate Security Policy
- Internet & E-Mail Security Policy
- Information Systems Terms of Use
- Compliance Policy

3.8 Compliance Measurement

Compliance with Virus and Malware policy is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.
• Compliance with Virus and Malware Policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
• Compliance measurement should also include periodic review for Security Quality Assurance.
• Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  ❖ Verbal or written warning
  ❖ Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

3.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>All Users / Manager Information Security</td>
</tr>
</tbody>
</table>

4 Password Policy

4.1 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information.

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should
contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.

4.2 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security.
- Custodians responsible for implementing this policy are listed in Section 4.8.

4.3 Definitions

Definition of some of the common terms:

**Authentication:** The identification requirements associated with an individual using a computer system. Identification information must be securely maintained by the computer system and can be associated with an individual's authorization and system activities. Three types of factors are used to provide authentication: a) Something you know (i.e., a password) b) Something you have (i.e., a certificate or smart card) c) Something you are (i.e., a fingerprint or retinal pattern).

**Availability:** Ensuring that authorized users have access to information and associated assets when required.

**Confidentiality:** Ensuring that information is accessible only to those authorized to have access.

4.4 Basic Assumptions

(None)

4.5 Policy Statements

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of KUWAIT UNIVERSITY’s entire corporate network. As such, all users of KUWAIT UNIVERSITY’s information systems (including employees, contractors, and vendors with access to KUWAIT UNIVERSITY systems) are
responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

4.5.1 Password Policy

4.5.1.1 General

4.5.1.1.1 All KUWAIT UNIVERSITY’s information systems must require identification and authentication through passwords, pass-phrases, one-time passwords and similar password mechanisms as a minimum (A more restrictive /secure authentication mechanism is acceptable) prior to allowing user access.

4.5.1.1.2 Passwords for KUWAIT UNIVERSITY systems must be created in accordance with this KUWAIT UNIVERSITY’s password policy (4.5.1.6.1).

4.5.1.1.3 KUWAIT UNIVERSITY’s information systems (access control programs) must be configured (where such configuration is possible) to fulfill the requirements of this policy and KUWAIT UNIVERSITY’s password rules, guidelines and procedures.

4.5.1.1.4 Passwords must be regarded as confidential information and must not be disclosed to any other person except in accordance with KUWAIT UNIVERSITY’s password management procedures for safekeeping of passwords.

4.5.1.1.5 Users are responsible and liable for all actions including transactions, information retrieval or communication on KUWAIT UNIVERSITY’s information systems performed by using their user-id(s) and password(s).

4.5.1.2 Validity Policy

4.5.1.2.1 All system-level and production environment passwords (e.g., root, NT admin, application administration accounts, etc.) must be changed every 30 days.

4.5.1.2.2 All user-level passwords (e.g., application user, email, web, desktop computer, etc.) must be changed at once every 90 days.
4.5.1.3 User Account Lock Out Policy

4.5.1.3.1 KUWAIT UNIVERSITY’s information systems must be configured (where this is possible) to lock the User-ID and prevent user access to the information system where an incorrect user password has been used 5 times in sequence.

4.5.1.3.2 KUWAIT UNIVERSITY’s information systems shall be configured (where this is possible) to automatically reinstate locked accounts after a defined period of at least 30 minutes. Otherwise; locked out user accounts must be reactivated in accordance with formal procedures developed and implemented to identify the user and determine the reason for the lockout.

4.5.1.4 Uniqueness Policy

4.5.1.4.1 User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

4.5.1.4.2 Password used for KUWAIT UNIVERSITY accounts must not be the same as passwords used for other non-KUWAIT UNIVERSITY access (e.g., personal ISP account, option trading, benefits, etc.).

4.5.1.4.3 Passwords must be checked to ensure that they are not identical to any of the previous passwords for the same account.

4.5.1.4.4 The same password must not be used for multiple KUWAIT UNIVERSITY access needs.

Description

For example, select different passwords for different information systems or operating systems.

4.5.1.5 Password Communication

4.5.1.5.1 Passwords must not be revealed in conversations, inserted into email messages or other forms of electronic communication unless it’s digitally signed and encrypted.
4.5.1.5.2 Passwords must not be written down, stored on any information system or storage device except in accordance with KUWAIT UNIVERSITY’s password management procedures for safekeeping of passwords.

4.5.1.5.3 Initial passwords must be communicated to users in a sealed envelope to be handed over on presentation of appropriate identification.

4.5.1.5.4 Initial passwords should only be valid for the first log-on attempt within a period of 48 hours from the time the password was handed over. Users must be forced to change the password on first use.

4.5.1.6 Composition

4.5.1.6.1 All user-level and system-level passwords must conform to the guidelines described below:

- User-level passwords must be at least 8 characters, while system-level passwords must be at least 12 alphanumeric characters long.
- System-level passwords must contain both upper and lower case characters (e.g., a-z, A-Z)
- Passwords must not be a dictionary word in any language, slang, dialect, jargon, etc.
- Passwords must not be based on personal information, names of family, date of births, etc.
- Passwords must NOT be the same as the username.

4.5.1.6.2 Password Confidentiality Guidelines:

- Passwords must never be written down or stored on-line. As far as possible, they should be easy to remember. For this purpose pass-phrase based passwords may be used.

Description

For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "Tmb1w2R!" or "Tmb1W>r~" or some other variation. (NOTE: Do not use either of these examples as passwords!)

- Passwords must not be revealed on any questionnaires or security forms.
- Passwords must not be revealed to family members or co-workers.
4.6 Related Information Security Policies

- Corporate Security Policy
- Access Control
- Compliance Policy

4.7 Compliance Measurement

Compliance with password policy is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

- Compliance Password Policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
- Compliance measurement should also include periodic review for Security Quality Assurance.
- Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  
  - Verbal or written warning
  - Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

4.8 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Manager Information Security / System and Network Administrators / All Users</td>
</tr>
</tbody>
</table>

5 Wireless Communication Policy

5.1 Purpose

This document sets out Kuwait University’s policy towards Wireless Communications
5.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Kuwait University's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Kuwait University's networks do not fall under the purview of this policy.

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.

5.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security
- Custodians responsible for implementing this policy are listed in Section 9

5.4 Definitions

Definition of some of the common terms:

**Critical**: Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

**Information Asset**: Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.
Sensitive: Concerned with highly classified information or involving discretionary authority over important official matters.

5.5 Basic Assumptions

(None)

5.6 Policy Statements

Register Access Points and Cards

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by InfoSec. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with InfoSec

Approved Technology

All wireless LAN access must use corporate-approved vendor products and security configurations.

VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.7 Related Information Security Policies

- Corporate Security Policy
- Internet & E-Mail Security Policy
- Asset Management Policy
- Access Control Policy

5.8 Compliance Measurement

Compliance with Information Communication, labeling and handling policy is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

- Compliance with Information Communication, labeling and handling policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
- Compliance measurement should also include periodic review for Security Quality Assurance.
- Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  - Verbal or written warning
  - Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

5.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>All Users / MANAGER INFORMATION SECURITY / IT DEPT.</td>
</tr>
</tbody>
</table>
6 Information Communication, Labeling, and Handling Policy

6.1 Purpose

This document sets out Kuwait University’s policy towards information communication, labeling and handling of its information assets

6.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.

6.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security
- Custodians responsible for implementing this policy are listed in Section 6.9

6.4 Definitions

Definition of some of the common terms:
Critical: Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

Information Asset: Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.

Sensitive: Concerned with highly classified information or involving discretionary authority over important official matters.

6.5 Basic Assumptions

(None)

6.6 Policy Statements

6.6.1 Information Labeling

6.6.1.1 General Controls

6.6.1.1.1 Stored information, both physical as well as electronic, should be labeled.

Description

Labeling systems should not be overcomplicated to ensure that the overhead does not outweigh the value of the items being protected.

6.6.1.1.2 Physical labeling of documents, hardware items and removable media should include appropriate security classifications in accordance with Kuwait University’s Asset Classification, Protection, Labeling & Handling Scheme and Information Labeling Procedure.

6.6.1.1.3 Electronic labeling for computer-based information should be introduced at folder level for sensitive and confidential information in accordance with Kuwait University’s Asset Classification, Protection, Labeling & Handling Scheme and Information Labeling Procedure.

6.6.1.1.4 Password controls and/or cryptography/check-summing for highly confidential information should be introduced.
6.6.1.2 Backup Media Labeling

6.6.1.2.1 Each backup media should be appropriately labeled with details of date, nature of backup (e.g. Full image copy or file copy), as well as classification label according to the Asset Classification, Protection, Labeling & Handling Scheme of KUWAIT UNIVERSITY.

6.6.1.2.2 All backup media should be labeled in accordance with Kuwait University’s Information Labeling Procedure as well as the procedures defined in the Naming Convention Guidelines.

6.6.1.3 Hard and Soft Document Labeling

6.6.1.3.1 All printed information, hardcopies and soft copies should be clearly labeled in accordance with the Asset Classification, Protection, Labeling & Handling Scheme, Kuwait University’s Information Labeling Procedure, Naming Convention Guidelines, Documentation Structure & Control document.

6.6.2 Information Handling

The Information Handling Procedures would identify controls over the storage and handling of information that will be consistent with the classification label assigned to the information (in accordance with the Asset Classification and Control Policy and associated procedures).

6.6.2.1 Information Handling Procedures

6.6.2.1.1 Information assets should be maintained, handled, stored, transported (or transmitted) and destroyed in accordance with Kuwait University’s Information Handling Procedures associated with the information asset’s classification label.

6.6.2.2 Management of Removable Computer Media

6.6.2.2.1 Media should be controlled and physically protected to prevent interruptions to business activities and damage to critical business information assets.
6.6.2.2 Removable computer media should be managed and controlled in accordance with applicable KUWAIT UNIVERSITY procedures.

6.6.2.3 Media should be stored in a safe and secure environment

6.6.2.4 Personnel who are not employees of KUWAIT UNIVERSITY departments, or contractors should not be able to identify critical business information assets by their labels.

6.6.2.5 The previous contents of any re-usable media should be completely erased.

6.6.2.3 Disposal of Media

6.6.2.3.1 Appropriate, secure, and safe disposal of critical business information assets should be in accordance with Kuwait University’s Information Handling Procedure.

Description

Media containing sensitive information should be disposed of securely and should be logged. All media items should be collected and disposed together. Adequate controls should be ensured while outsourcing disposal of media. The disposal procedures must cover all media including hardcopy materials, carbon paper, one-time-use printer or fax ribbons, magnetic tapes, removable disks or cassettes, etc.

6.6.2.4 Secure Disposal or Re-Use of Equipment

6.6.2.4.1 All equipment containing storage media (e.g., fixed hard drives) should be checked to ensure that any critical business information assets and licensed software are removed, securely overwritten or destroyed prior to disposal.

6.6.2.4.2 Before any KUWAIT UNIVERSITY owned or managed hard disk or magnetic media or system containing a storage media is transferred, surpluses, or donated, it should be sanitized by reformatting the hard drive in a secure manner or by using an approved wipe-out utility.
6.6.2.4.3 Diskettes and other magnetic storage media that contain any corporate data or software should be sanitized when they are no longer needed.

6.6.2.4.4 Portable media should only be reused after overwriting or degaussing. Otherwise, it should be destroyed once no longer needed.

6.6.2.4.5 Information systems and hard disks sent outside KUWAIT UNIVERSITY for repair or data recovery should be protected from disclosure by contract with the company performing the service.

Description

Some methods of secure disposal of media are described below:

- Physically destroying the drive, rendering it unusable.
- Degaussing the drive to randomize the magnetic domains - most likely rendering the drive unusable in the process.
- Overwriting the drive’s data so that it cannot be recovered.

6.6.2.5 Security of System Documentation

6.6.2.5.1 System documentation should be protected from unauthorized access

6.6.2.5.2 The system or application owner should authorize or approve distribution lists for system documentation. This list should be restricted to a minimum number of parties.

6.6.2.5.3 Access to documentation that supports the KUWAIT UNIVERSITY departments, and which is used by programming, operations and user personnel, should be restricted to personnel performing official duties

6.6.2.6 Removal of Documents or files

6.6.2.6.1 Removal should be authorized by a supervisor (or equivalent) who should be satisfied that the removing person is aware of the potential risks involved and that he / she is responsible for its safe custody at all times.
6.6.2.7 Copying, Storage and Disposal

6.6.2.7.1 Confidential hardcopy and any form of unencrypted removable electronic media should be held in a secure container or a secure area.

6.6.2.7.2 Outdated confidential paper information should be shredded by the owner.

6.6.2.8 Manual Transmission

6.6.2.8.1 Manual transmission of soft and hard information should be protected from unauthorized disclosure or access by adopting adequate safeguards.

Description

Some methods are as follows:

- Using single opaque envelope that indicates the classification.
- Receipt at discretion of originator either passed by hand between people who have the ‘need to know’ or placed in locked container and delivered direct, by hand or by an authorized messenger.

6.6.2.9 Clear Desk Policy

6.6.2.9.1 KUWAIT UNIVERSITY employees should follow a clear desk policy for papers and removable storage media in order to reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours.

6.6.2.9.2 The items with sensitive labels should be secured when unattended and their content always unobservable to people without the ‘need to know’.

Description

Guidelines should be developed and implemented to promote Kuwait University’s clear desk policy. These could include the following:

- Paper and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.
• Sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.
• Personal computers and computer terminals and printers are not to be left logged on when unattended and should be protected by password protected screen savers.
• Sensitive or classified information, when printed, is to be cleared from printers immediately.

6.6.3 Information Transmission / Communication Handling

To prevent loss, modification, destruction, or misuse of information, KUWAIT UNIVERSITY departments should protect and control exchange of critical business information assets and software.

6.6.3.1 Information and Software Exchange Agreements

6.6.3.1.1 Formal agreements should be established for the exchange of critical business information assets or software with outside organizations. The department requiring this exchange should be responsible for the formal agreements.

6.6.3.1.2 These agreements should include both manual and electronic exchanges.

6.6.3.1.3 These agreements should reflect the sensitivity of the critical business information assets being exchanged and should describe any protection requirements.

6.6.3.1.4 These agreements must specify management responsibilities, notification requirements, packaging and transmission standards, courier identification, responsibilities and liabilities, data and software ownership, protection responsibilities and measures, and all encryption requirements.
6.6.3.2 Information Exchange through Fax Machines

6.6.3.2.1 Sensitive or confidential information should only be faxed where a more secure means of communication is not available. Both the sender of the information and the intended recipient should authorize the transmission of the information before the transmission.

6.6.3.2.2 All fax messages should include a confidentiality clause prohibiting the recipient from disclosing the information if such a fax is received in error.

6.6.3.2.3 Any fax received in error should be destroyed and its sender notified - if this is possible.

6.6.3.3 Information Exchange through Electronic Mail

6.6.3.3.1 Precautions must be taken to safeguard privacy of KUWAIT UNIVERSITY employees, as well as any third party users (e.g. customers and vendors), who use the email systems.

6.6.3.3.2 The purpose for which the email system is to be used (such as business only or personal use) should be authorized by the relevant management.

6.6.3.3.3 Penalties for misuse of email system should be defined and imposed on persons found in misuse of the system.

6.6.3.3.4 Persons who can access email messages of the employee on temporary but extended leave should be authorized.

6.6.3.3.5 The retention/purge schedule for files should be defined and implemented.

6.6.3.3.6 Password creation and change procedures for email systems should be in accordance with Kuwait University’s Password Policy.

6.6.3.3.7 Encryption or other means of protecting information sent through emails should be employed while sending sensitive information by email.
6.6.3.3.8 Safeguards concerning copying and forwarding messages, especially messages containing personally identifiable data should be defined and implemented.

6.6.4 Portable Computer and Work-at-Home Situations

6.6.4.1 Portable Computer and Work-at-Home Situation

6.6.4.1.1 Personally identifiable information on portable computers and hand-held personal organizers should be safeguarded when transported outside of KUWAIT UNIVERSITY by employees.

6.6.4.1.2 For KUWAIT UNIVERSITY employees who work at home, including temporary and contract staff, procedures and training programs should emphasize responsible information-handling practices.

6.6.4.1.3 The network connection between home and work should be secure (e.g. dial-back facility or secure identification tokens).

6.7 Related Information Security Policies

- Corporate Security Policy
- Internet & E-Mail Security Policy
- Asset Management Policy
- Access Control Policy

6.8 Compliance Measurement

Compliance with Information Communication, labeling and handling policy is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

- Compliance with Information Communication, labeling and handling policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
- Compliance measurement should also include periodic review for Security Quality Assurance.
- Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
- Verbal or written warning
- Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

### 6.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>All Users / MANAGER INFORMATION SECURITY / IT DEPT.</td>
</tr>
<tr>
<td>6.2</td>
<td>All Users / MANAGER INFORMATION SECURITY/IT DEPT./IT User Support</td>
</tr>
<tr>
<td>6.3</td>
<td>All users / IT DEPT.</td>
</tr>
<tr>
<td>6.4</td>
<td>Business Heads / IT DEPT.</td>
</tr>
<tr>
<td>6.5</td>
<td>All Users</td>
</tr>
</tbody>
</table>

### 7 LDAP Policy

#### 7.1 Purpose

This document sets out Kuwait University’s policy towards LDAP

#### 7.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.
7.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security
- Custodians responsible for implementing this policy are listed in Section 7.9

7.4 Definitions

Definition of some of the common terms:

**Critical:** Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

**Information Asset:** Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.

**Sensitive:** Concerned with highly classified information or involving discretionary authority over important official matters.

7.5 Basic Assumptions

(None)

7.6 Policy Statements

**Directory Services**

KU will maintain a standard LDAP Directory Service.

**Function**

Maintain contact, role and course details for all staff and students at the University. VPN Encryption and Authentication

Act as a central collection point for sets of data about people, departments, courses or any other data sets which are important to the running of the University.
Support for any application which required LDAP and which is of general use to the University. Example - Internet connectivity

Implement any data storage/retrieval requirement for which LDAP access is a viable solution.

**Authentication**

Authentication will be by Kerberos.

LDAP passwords will still be supported for legacy systems, such as the company name, division title, employee name, or product identifier.

### 7.7 Related Information Security Policies

- Corporate Security Policy
- Internet & E-Mail Security Policy
- Asset Management Policy
- Access Control Policy

### 7.8 Compliance Measurement

Compliance with Information Communication, labeling and handling policy is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

- Compliance with Information Communication, labeling and handling policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
- Compliance measurement should also include periodic review for Security Quality Assurance.
- Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  - Verbal or written warning
  - Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

### 7.9 Custodians

<table>
<thead>
<tr>
<th>Policy</th>
<th>Custodian</th>
</tr>
</thead>
</table>

KUWAIT UNIVERSITY © 2015
8 Network Servers Policy

8.1 Purpose

The purpose of this policy is to establish a set of roles and requirements to control all servers connected to KUWAIT UNIVERSITY’s demilitarized networks (DMZ) which has servers published on the internet. It is also to establish standards for the base configuration of internal server equipment that is owned and/or operated by KUWAIT UNIVERSITY. Effective implementation of this policy will minimize unauthorized access to KUWAIT UNIVERSITY proprietary information and technology.

8.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information.

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.
8.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security.
- Custodians responsible for implementing this policy are listed in Section 8.9.

8.4 Definitions

Definition of some of the common terms:

**Critical:** Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

**Information Asset:** Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.

**Sensitive:** Concerned with highly classified information or involving discretionary authority over important official matters.

**Availability:** Ensuring that authorized users have access to information and associated assets when required.

8.5 Basic Assumptions

(None)

8.6 Policy Statements

8.6.1 Network Servers Requirements

8.6.1.1 General Controls

8.6.1.1.1 Each Server on the network should be connected to one subnet only.

8.6.1.1.2 Any Server on the network should have KUWAIT UNIVERSITY Official Antivirus System, it should be updated with the latest updates and virus definition file.
8.6.1.1.3 Any Server on the network should have a Security Agents (e.g. Enterprise System Management (ESM) and Intruder Alert (ITA))

8.6.1.1.4 Any Server on the network should be updated with the latest OS patches, updates, service packs and Security Updates etc.

Description:
Test this Patches for compatibility with the applications and systems running on the platform in a test environment prior to implementation in the production /live environment.

8.6.1.1.5 Each Server to be installed on the network should use Static IP address provided by Network Team after completion of the general controls as addressed in 6.1.1.2 - 1.4

8.6.1.1.6 Anti Virus and security agents should be running, stopping such service without prior notification is totally prohibited.

8.6.1.1.7 Information Security Standards should be applied on the Operating System and Database installed on the server.

8.6.1.1.8 Processes that are not required specifically to the operation of the servers should be deactivated / disabled.

8.6.1.1.9 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using IPSEC VPN).

8.6.1.1.10 All local management of the devices should be done via secure protocols like SSH and SFTP and not telnet or FTP.

8.6.1.1.11 Any server should join a known and trusted domain and Server Administrators should provide their server(s) information to Network Security Team periodically

Description:
Manager Information Security will request for example Server IP, Owner Dept., Backup Administrator(s) etc. for incident responding procedure so they can contact the right person if such incident occurs.

8.6.1.2 General Configuration Guidelines

8.6.1.2.1 Operating System configuration running on the network servers should be in accordance with Minimum Baseline Security Standard (MBSS) documents.

8.6.1.2.2 Services and applications that will not be used should be disabled where practical.

8.6.1.2.3 Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

8.6.1.2.4 The most recent security patches should be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

8.6.1.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Use a trust relationship should be avoided, when some other method of communication will work.

8.6.1.2.6 Use of root account should be avoided

8.6.1.2.7 All systems should adhere to the Password Policy.

8.6.1.2.8 Accounts without password should be eliminated immediately.

8.6.1.2.9 All default accounts (shipped with the OS) should be disabled.

8.6.1.2.10 In case the responsibilities of the system is changed (e.g. administrator has been changed), accordingly the relevant account credentials should be changed immediately.

8.6.1.2.11 Users belong to administrators group should be managed and minimized to what is required (Least Privilege).
8.6.1.2.12 Server Administrators should access their servers in a controlled manner via secured link.

8.6.1.2.13 Server Administrators should have separate account(s) for non-administrative task(s).

8.6.1.2.14 User Accounts should be subject to periodic review (each three months) by the Server Administrators.

8.6.1.2.15 Temporary accounts, vendor accounts and contractor accounts validity period should be determined earlier when creating such accounts.

8.6.1.3 Logs Manipulation and Monitoring

8.6.1.3.1 Access logs should be subject to periodic review (on monthly basis) by the network owner.

8.6.1.3.2 Log files can be accessed only by System Administrators.

8.6.1.3.3 Access Logs shall be archived for a maximum period of six months, then it should be destroyed in a secure manner, Manager Information security head should approve such disposal of information.

8.6.1.3.4 All security-related events on critical or sensitive systems should be logged and audit trails saved as follows:

- All security related logs shall be kept online for a minimum of 1 week.
- Daily incremental tape backups shall be retained for at least 1 month.
- Weekly full tape backups of logs shall be retained for at least 1 month.
- Monthly full backups shall be retained for a minimum of 2 years.

8.6.1.3.5 Security-related events will be reported to Manager Information Security, who will review logs and report incidents to management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
• Anomalous occurrences that are not related to specific applications on the host

8.7 Related Information Security Policies

• Corporate Security Policy
• Communications & Operations Management Policy
• Access Control Policy
• Backup & Restoration Policy
• Password Policy

8.8 Compliance Measurement

Compliance with Network Servers Policy is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

• Compliance with Network Servers Policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
• Compliance measurement should also include periodic review for Security Quality Assurance.
• Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  
  ❖ Verbal or written warning
  ❖ Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

8.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Manager Information Security / IT DEPT.</td>
</tr>
</tbody>
</table>
9 Network Servers Policy

9.1 Purpose

The purpose of this policy is to establish a set of roles and requirements to control all servers connected to KUWAIT UNIVERSITY's demilitarized networks (DMZ) which has servers published on the internet. It is also to establish standards for the base configuration of internal server equipment that is owned and/or operated by KUWAIT UNIVERSITY. Effective implementation of this policy will minimize unauthorized access to KUWAIT UNIVERSITY proprietary information and technology.

9.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information.

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.

9.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security.
- Custodians responsible for implementing this policy are listed in Section 9.9.
9.4 Definitions

Definition of some of the common terms:

**Critical:** Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

**Information Asset:** Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.

**Sensitive:** Concerned with highly classified information or involving discretionary authority over important official matters.

**Availability:** Ensuring that authorized users have access to information and associated assets when required.

9.5 Basic Assumptions

(None)

9.6 Policy Statements

9.6.1 Network Servers Requirements

9.6.1.1 General Controls

9.6.1.1.1 Each Server on the network should be connected to one subnet only.

9.6.1.1.2 Any Server on the network should have KUWAIT UNIVERSITY Official Antivirus System, it should be updated with the latest updates and virus definition file.

9.6.1.1.3 Any Server on the network should have a Security Agents (e.g. Enterprise System Management (ESM) and Intruder Alert (ITA))

9.6.1.1.4 Any Server on the network should be updated with the latest OS patches, updates, service packs and Security Updates etc.
Description:
Test this Patches for compatibility with the applications and systems running on the platform in a test environment prior to implementation in the production/live environment.

9.6.1.1.5 Each Server to be installed on the network should use Static IP address provided by Network Team after completion of the general controls as addressed in 6.1.1.2 - 1.4

9.6.1.1.6 Anti Virus and security agents should be running, stopping such service without prior notification is totally prohibited.

9.6.1.1.7 Information Security Standards should be applied on the Operating System and Database installed on the server.

9.6.1.1.8 Processes that are not required specifically to the operation of the servers should be deactivated/disabled.

9.6.1.1.9 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using IPSEC VPN).

9.6.1.1.10 All local management of the devices should be done via secure protocols like SSH and SFTP and not telnet or FTP.

9.6.1.1.11 Any server should join a known and trusted domain and Server Administrators should provide their server(s) information to Network Security Team periodically

Description:
Manager Information Security will request for example Server IP, Owner Dept., Backup Administrator(s) etc. for incident responding procedure so they can contact the right person if such incident occurs.

9.6.1.2 General Configuration Guidelines

9.6.1.2.1 Operating System configuration running on the network servers should be in accordance with Minimum Baseline Security Standard (MBSS) documents.
9.6.1.2.2 Services and applications that will not be used should be disabled where practical.

9.6.1.2.3 Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

9.6.1.2.4 The most recent security patches should be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

9.6.1.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Use a trust relationship should be avoided, when some other method of communication will work.

9.6.1.2.6 Use of root account should be avoided

9.6.1.2.7 All systems should adhere to the Password Policy.

9.6.1.2.8 Accounts without password should be eliminated immediately.

9.6.1.2.9 All default accounts (shipped with the OS) should be disabled.

9.6.1.2.10 In case the responsibilities of the system is changed (e.g. administrator has been changed), accordingly the relevant account credentials should be changed immediately.

9.6.1.2.11 Users belong to administrators group should be managed and minimized to what is required (Least Privilege).

9.6.1.2.12 Server Administrators should access their servers in a controlled manner via secured link.

9.6.1.2.13 Server Administrators should have separate account(s) for non-administrative task(s).

9.6.1.2.14 User Accounts should be subject to periodic review (each three months) by the Server Administrators.
9.6.1.2.15 Temporary accounts, vendor accounts and contractor accounts validity period should be determined earlier when creating such accounts.

9.6.1.3 Logs Manipulation and Monitoring

9.6.1.3.1 Access logs should be subject to periodic review (on monthly basis) by the network owner.

9.6.1.3.2 Log files can be accessed only by System Administrators.

9.6.1.3.3 Access Logs shall be archived for a maximum period of six months, then it should be destroyed in a secure manner, Manager Information security head should approve such disposal of information.

9.6.1.3.4 All security-related events on critical or sensitive systems should be logged and audit trails saved as follows:

  - All security related logs shall be kept online for a minimum of 1 week.
  - Daily incremental tape backups shall be retained for at least 1 month.
  - Weekly full tape backups of logs shall be retained for at least 1 month.
  - Monthly full backups shall be retained for a minimum of 2 years.

9.6.1.3.5 Security-related events will be reported to Manager Information Security, who will review logs and report incidents to management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host

9.7 Related Information Security Policies

  - Corporate Security Policy
  - Communications & Operations Management Policy
  - Access Control Policy
  - Backup & Restoration Policy
  - Password Policy
9.8 Compliance Measurements

Compliance with Network Servers Policy is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

- Compliance with Network Servers Policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
- Compliance measurement should also include periodic review for Security Quality Assurance.
- Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  - Verbal or written warning
  - Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

9.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Manager Information Security / IT DEPT.</td>
</tr>
</tbody>
</table>

10 Employee Exit Policy

10.1 Purpose

The purpose of this policy is to reduce risk with respect to Confidentiality, Integrity and Availability (CIA) of KUWAIT UNIVERSITY information assets from an employee, contractor or other third party service provider who exits KUWAIT UNIVERSITY or is voluntarily terminated. This document relates to Kuwait University’s policy towards such employees, contractors and other third party service providers.

10.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.
This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information.

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.

10.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security.
- Custodians responsible for implementing this policy are listed in Section 9.

10.4 Definitions

Definition of some of the common terms:

**Critical**: Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

**Information Asset**: Any resource of information which has a value to the organization, it can be any system or component, hardware, software, database or facility.

**Sensitive**: Concerned with highly classified information or involving discretionary authority over important official matters.

10.5 Basic Assumptions

(Nothing)
10.6 Policy Statements

10.6.1 Exit Policies

10.6.1.1 Withdrawal of Access rights on Termination of an Employee, Contractor or Third party Service Provider

10.6.1.1.1 On termination of an employee, contractor or third party service provider:

- All information systems accesses must be revoked effective the date of issuance of termination orders
- The concerned party’s physical access to Kuwait University’s internal facilities should be withdrawn immediately.

10.6.1.2 Recovery of IT Assets and Equipments

10.6.1.2.1 On termination of an employee, contractor or third party service provider, all information systems assets issued to the concerned person must be recovered with immediate effect and prior to settlement of dues and departure from the organization.

10.6.1.3 Withdrawal of Access Rights on Resignation / Voluntary Termination of Employment, Completion of Contractual Obligation or Services

10.6.1.3.1 Upon notification of staff resignations, HUMAN RESOURCES should in consultation with MANAGER INFORMATION SECURITY and concerned department head, assess whether the staff’s continued access to information systems poses a risk to the organization. If so, access rights should be revoked immediately.

10.6.1.3.2 On resignation / voluntary retirement of employment, completion of contractual obligations or services:

- All information systems access must be revoked on the date of settlement of dues or date of departure from the organization (whichever is earlier)
- The concerned party’s physical access Kuwait University’s internal facilities must be withdrawn and restricted effective on the date of...
settlement of dues or date of departure from the organization (whichever is earlier)

10.6.1.4 Exit Interviews

10.6.1.4.1 All employees should be interviewed before their departure from the organization, and details (e.g., Obligations of Non-Disclosure) of the interviews should be documented for future reference.

10.7 Related Information Security Policies

- Internet & E-Mail Security Policy
- Password Policy
- Access Control Policy
- Compliance Policy
- HR termination policies and procedures

10.8 Compliance Measurement

KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

- Compliance with Employee Exit Policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
- Compliance measurement should also include periodic review for Security Quality Assurance.
- Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  - Verbal or written warning
  - Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

10.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>HUMAN RESOURCES / MANAGER</td>
</tr>
<tr>
<td></td>
<td>INFORMATION SECURITY / Department</td>
</tr>
</tbody>
</table>
11 Backup and Restoration Policy

11.1 Purpose

This document sets out Kuwait University’s policy towards taking backups of its information assets, including their frequency, storage, retention, documentation and restoration.

11.2 Scope

This policy applies to all users of information assets at KUWAIT UNIVERSITY regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by KUWAIT UNIVERSITY or contracted with a third party by KUWAIT UNIVERSITY. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, and wireless devices), software, and information

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other KUWAIT UNIVERSITY Information Security policies, standards and procedures define additional responsibilities. All users are required to read, understand and comply with this Information Security policy. If any user requires further clarifications on this policy, he/she should contact the line manager, IS HELPDESK, or the MANAGER INFORMATION SECURITY.

Manager Information Security and the concerned department/division units shall jointly resolve any conflicts arising from this policy.
11.3 Responsibilities

- The Manager Information Security is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be directed to Manager Information Security
- Custodians responsible for implementing this policy are listed in Section 12.9

11.4 Definitions

Definition of some of the common terms:

**Authentication:** The identification requirements associated with an individual using a computer system. Identification information must be securely maintained by the computer system and can be associated with an individual's authorization and system activities. Three types of factors are used to provide authentication: a) Something you know (i.e., a password) b) Something you have (i.e., a certificate or smart card) c) Something you are (i.e., a fingerprint or retinal pattern).

**Availability:** Ensuring that authorized users have access to information and associated assets when required.

**Confidentiality:** Ensuring that information is accessible only to those authorized to have access.

11.5 Basic Assumptions

(None)

11.6 Policy Statements

11.6.1 Backup & Restoration

11.6.1.1 General

**11.6.1.1 Back up of business information (data) and software should be taken according to a comprehensive schedule based on the business requirement for the specific application/system.**
11.6.1.1.2 Adequate back-up facilities should be provided to ensure that all essential business information and software could be recovered following a disaster or media failure.

11.6.1.1.3 Back-up arrangements for individual systems and related data should be tested according to a formal schedule to ensure that they meet the requirements of business continuity plans.

11.6.1.2 Backup & Restoration

11.6.1.2.1 All applications, operating systems, data (including databases), user configuration information and hardware configuration information (where applicable) must be backed up in accordance with the Backup and Restoration Procedure.

11.6.1.2.2 Separate systems specific backup and restoration procedures must be developed in accordance with system requirements and vendor recommendations. These procedures must be documented and implemented during (and as part of) system implementation.

Description

The Backup and Restoration Procedure will determine the type of backups to be performed, the periodicity or schedule of the backup, the protection to be provided to backup media. The level of protection will be based on the criticality of the information backed up as determined by Kuwait University’s Asset Classification and Control Policy and Asset Classification, Protection, Labeling & Handling Scheme.

11.6.1.2.3 Restoration of backups will require specific and appropriate authorization and must be performed in accordance with the Backup and Restoration Procedure.

11.6.1.2.4 Systems Administrators shall perform a verification process on the back-up data to make sure that it is backed up successfully.

11.6.1.2.5 Systems Administrators shall perform a backup before and after installing batches or upgrades or making any configuration changes on the system.
11.6.1.2.6  Backed up data that is confidential must be stored in encrypted form.

11.6.1.3  Testing

11.6.1.3.1  Systems Administrators must check the quality of the back up media (tapes, floppy diskettes, CDs, etc.) regularly and make sure that they are in a good condition to be re-used.

11.6.1.3.2  After completion of backup testing, all data must be safely erased from the test environment.

11.6.1.3.3  The System Administrator is responsible for testing system software and data backups by restoring a sample of the backups according to a formal schedule in the test environment. The logs and records should be maintained and sent to the Manager Information Security for review and record keeping.

11.6.1.3.4  Restoration procedures must be regularly checked (at least once a year) and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

11.6.1.4  Backup Frequency

11.6.1.4.1  The frequency of data backup for each system must be determined by considering the ‘Availability’ and ‘Integrity’ criteria in accordance with Kuwait University’s Asset Classification, Protection, and Labeling & Handling Scheme.

11.6.1.4.2  At least three generations or cycles of back-up information must be retained for important business applications and critical data of KUWAIT UNIVERSITY.

11.6.1.4.3  Additional number of generations or cycles of backup must be determined by taking into account the criticality and specific requirements of different systems.

11.6.1.4.4  Daily and weekly backup tapes must be stored near the correspondent information system site server computer (on-site storage) to be readily available.
11.6.1.5 Off Site Storage

11.6.1.5.1 Backup tapes must be stored off-site at a periodicity according to data criticality in order to be available in the event of a disaster, or for long-term storage.

11.6.1.5.2 A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, must be stored in a remote location, at a sufficient distance from Kuwait University’s Data Center and other processing facilities to escape any damage from a disaster at the main site.

11.6.1.5.3 At least two copies of fully recoverable version of all “critical” data must be made. One copy must be stored at the Data Center or the main processing facility whereas the other copy must be stored at an off-site storage location.

11.6.1.6 Physical & Environmental Controls

11.6.1.6.1 Back-up media must be given an appropriate level of physical and environmental protection consistent with the standards applied at the Data Center or a main processing facility. The controls applied to media at the Data Center or a main processing facility must also be implemented at the back-up site.

11.6.1.7 Backup Retention

11.6.1.7.1 Backups of all KUWAIT UNIVERSITY data must be retained such that all systems are fully recoverable. At a minimum, each backup must be retained for 30 days.

11.6.1.7.2 The retention period and any requirement for archive copies to be retained for longer periods (or permanently) must be formally determined for critical business information as well as based on any legal requirements.
11.6.1.8 Documentation

11.6.1.8.1 Backup documentation must include identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.

11.6.1.8.2 Each backup media must be appropriately labeled with details of owner, date, nature of backup (e.g. Full image copy or file copy). In addition, it must be given a classification label, as applicable, according to Kuwait University’s Information Labeling Procedure.

11.6.1.8.3 The movement of any backup media between the Data Center, the main processing facility and the offsite location must be logged.

Description

The on-site backup media log must contain the following information:

- Date of taking the backup.
- Date of moving the media to the offsite location
- Contents of the media (e.g. transaction backup, application backup, entire system backup)
- Nature of backup (e.g. full image copy or file copy)
- Name of the Carrier
- Name of the off-site location
- Name and signature of the responsible person at the on-site location
- Any other label information

11.6.1.8.4 Documentation of the restoration process must include procedures for the recovery from single-system or application failures as well as for a total KUWAIT UNIVERSITY Data Center or main processing facilities disaster scenario.

11.6.1.8.5 Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
11.6.1.9 Determining factors influencing backup

11.6.1.10 Specifying the data to be backed up

11.6.1.10.1 The data of the IT system (IT application) required to be backed up must be determined.

Description

This includes the application and operational software, system data (e.g. initialization files, macro definitions, configuration data, text blocks, password files, and access-right files), the application data as such and the protocol data (such as that relating to log-ins and data transmissions).

11.6.1.11 Data Availability requirements of IT systems

11.6.1.11.1 The availability requirements for the data must be stipulated.

Description

A proven standard like the maximum permissible downtime specifies the time period during which the specialized task can be performed without the availability of the relevant data and without the need for resorting to backup copies.

11.6.1.11.2 Consideration must also be given as to whether paper usage would allow short-term continuation of operations without IT support.

11.6.1.12 Modification Volumes

11.6.1.12.1 The volume of data that is modified over a certain time period must be considered while establishing the frequency of data backup.

11.6.1.13 Modification Times

11.6.1.13.1 Where data is modified continuously in a system, an appropriate data backup frequency must be specified.
11.6.1.14  Deadlines

11.6.1.14.1  It must be determined whether certain deadlines have to be observed for the data. This can involve storage or deletion deadlines relating to person-related data.

11.6.1.14.2  These deadlines must be considered when laying down the system specific data backup policies.

11.6.1.15  CIA Requirements

11.6.1.15.1  Consideration must be given as to the confidentiality requirements of the data needing backup.

11.6.1.15.2  Data backups must ensure that data are stored integrally and not modified during the period of storage.

11.6.1.16  Guidelines

11.6.1.16.1  The Data backup system guideline must be referenced when selecting a backup system.

11.7 Related Information Security Policies

- Corporate Security Policy
- Access Classification and Handling Policy
- Information Labeling and Handling Policy
- Physical and Environmental Security Policy
- Communication and Operations Management Policy
- Compliance Policy

11.8 Compliance Measurements

Compliance Backup and Restoration is mandatory. KUWAIT UNIVERSITY managers must ensure continuous compliance monitoring within their organization.

- Compliance with Backup and Restoration Policy will be matter for periodic review by Audit Division as per the audit guidelines and procedures.
• Compliance measurement should also include periodic review for Security Quality Assurance.
• Violations of the policies, standards and procedures of KUWAIT UNIVERSITY will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not limited to:
  ❖ Verbal or written warning
  ❖ Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

11.9 Custodians

<table>
<thead>
<tr>
<th>Policy Reference</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>System Administrators / IT Ops and support Dept.</td>
</tr>
<tr>
<td>6.2</td>
<td>BCP / IT Ops and Support Dept</td>
</tr>
<tr>
<td>6.3</td>
<td>IT Ops and Support Dept</td>
</tr>
<tr>
<td>6.4</td>
<td>All Users</td>
</tr>
</tbody>
</table>