



King Faisal University

Deanship of Information Technology

Acceptable Use Policy for Information Systems

[Chapter 07 section 3 of Information Security Framework and
Policies]

VERSION 1.0 (MAY 2011)

VERSION 2.0 (REVIEWED IN JUNE 2012)

Document Control Information

Document Details	
Document Name	EN - KFU-DIT-ISP-07-3-AUP Acceptable Use Policy 2011 v 2.0
Purpose of Document	Establish eligibility and acceptable use policy under the Information Security Framework and Policies of the King Faisal University. Being a sub policy under the chapter 7 section 3 (Asset Management Policy) of the Information Security Policy (ISP Manual) of the KFU; this part is dealing with the 'Protection of Information Assets and Responsibility for Information Assets.
Document Version Number	2011 v1.0 (Initial) 2011 v2.0 (Reviewed)
Document Status	Live
Document Owner	Dean of Information Technology
Prepared By	M. Shahul Hameed, MBA, M.Sc., CMA, CIA, PMP, CISA, ITIL, Advisor to Dean & Head of Quality Management Office, Deanship of Information Technology
Date of First Draft	May 2011
Date Approved	Oct 2011
Approved By	Dean of IT & VP For Development and Community Services (email on 24-11-2011)
Next Scheduled Review Date	May 2013
Classification	Public
Number of Pages / File Size	24 pages

Document Change History & Version Control

Function	Name	Title	Version	Signed Date
Prepared by (Initial draft proposal)	M. Shahul Hameed	Advisor to Dean & Head of Quality Management Office, Deanship of IT	V 1.0	10-10-2011
Review by	Peers	Deanship of Quality Assurance & Academic Accreditation	V 1.0	23-11-2011
Validated & Approved by	Dr. Mohammed S. Al-Zahrani	Dean of Information Technology	V 1.0	24-11-2011
Approved by	Dr. Ahmed A. Al-Shoaibi	Vice President For Development & Community Service	V 1.0	24-11-2011
Distributed to	All KFU Deanship and Departments	"For Internal & External Communication" – to be published through the website		Published on the web site on 29-11-2011
Assisted by (ARABIC translation)	Ahmed Samir. Morsy, and Arabic Translation Teamwork	Quality Management Office - Deanship of IT	V 2.0	27-06-2012
Adding Illustrative drawings and Graphics	Vadde Chattanya Sarath	Quality Management Office - Deanship of IT	V 2.0	27-06-2012

Validated v 2.0	M. Shahul Hameed	Advisor to Dean & Head of Quality Management Office, Deanship of IT	V 2.0	
Approved v 2.0	Dr. Mohammed S. Al-Zahrani	Dean of Information Technology	V 2.0	

Table of Contents

Document Control Information	2
Document Change History & Version Control	3
Table of Contents	5
Chapter 7.3 : Acceptable Use Policy for Information Systems of KFU	6
1. Overview	6
2. Purpose	7
3. Scope	7
4. Related References	7
4.1. References	7
5. Policy	8
5.1. General Use and Ownership.....	8
5.2. Use of Classified and Proprietary Information.....	8
5.3. Use of Information classified as "CONFIDENTIAL" or above.....	11
5.4. Unacceptable Use.....	12
5.5. Limited Personal Use of Information & Communication Systems	15
5.6. Communication via Internet, E-mail, and Blogging.....	16
5.7. Installation and modification of Software and Electronic Equipment	18
5.8. Accessing Files of other Users, Unauthorized access attempts & Disk Sharing.....	19
5.9. Encryption Keys & Passwords	20
5.10. Mobile computing / Teleworking and Using them in Public places.....	21
5.11. Incident and Weakness Reporting	22
6. Disciplinary Actions and KFU Rights	24

Chapter 7.3: Acceptable Use Policy for Information Systems of KFU

1. Overview

The King Faisal University (KFU) owns and operates information technology and related systems that are made available to users for supporting its operations. Thus the granting of access to KFU network and its other information technology related resources as provided to its community carries certain responsibilities and obligations as to what constitutes acceptable use or fair use of the KFU network.

This is a sub policy under the King Faisal University's Information Security Framework & Policies and is being referred as chapter 7.3 in its compiled policy manual for explaining how KFU information technology resources are to be used and specifies what actions are prohibited.

While this policy is as complete as possible, no policy can cover every situation, and therefore the user is asked additionally to use common sense when using the KFU resources. Questions on what constitutes acceptable use or fair use should be directed to the user's supervisor. Section 4 (Glossary of Important Terms) of this policy manual, covers additional information that might be helpful for the understanding of certain key technical terms used. For further assistance, the IT coordinator of each deanship/department can contact the Quality Management Office of the Deanship of Information Technology (KFU/DIT/QMO), who will provide such guidance or assistance that might be required to provide additional clarification for any new situation.


All internal and external users of the KFU resources should use them in an efficient, ethical and legal manner. It is to be understood that though the professional codes of conduct may seem strict, they are in place to protect the public and ensure its safety. Therefore, a strong security culture must be established by involvement and commitment of all stakeholders.

2. Purpose

The key objective of this policy is the protection of information assets of the KFU. Since inappropriate use of KFU systems exposes the university and society to risk, it is important to specify exactly what is permitted and what is prohibited.

This policy, therefore, gives the KFU community the details of the acceptable use or fair use and sets the principles and rules for the proper use of information and related technology resources of KFU.

3. Scope

 ***please refer to section 1.3 Scope of the KFU-DIT-ISP Information Security Framework and Policy Manual.***

4. Related References

4.1. References

 ***please refer to section 1.6 related references of the KFU-DIT-ISP***

Information Security Framework and Policy (ISP manual) for more detailed references information relating to relevant policies, procedures and/or guidelines in order to gain a more comprehensive approach and understanding.

Interpretations and important rules that are applicable to public use shall be made available through the KFU-DIT's website

www.kfu.edu.sa/ar/Deans/it/Pages/Home.aspx (for Arabic) and

www.kfu.edu.sa/en/Deans/it/Pages/Home.aspx (for English).

Other useful sub policies that are related to this sub policy are the following ***and please refer to:***

- a)  ***Chapter 7.1 Responsibility for Assets: Inventory Control***

5. Policy

5.1. General Use and Ownership

- 5.1.1. All users of information systems should comprehend the need for protecting the university information and perform their daily activities in compliance with the King Faisal University's Information Security Framework (the policies, standards, guidelines and relevant procedures).
- 5.1.2. While KFU's Deanship of Information Technology (KFU/DIT), through its network administration team, desires to provide a reasonable level of privacy, users should be aware that the data they create on the KFU systems remains the property of KFU. Because of the need to protect KFU's network, management cannot guarantee the confidentiality of information stored on any network device belonging to KFU.
- 5.1.3. For security and network maintenance purposes, authorized individuals within KFU may monitor information systems and network traffic at any time or continuously as per the Information Security Audit requirement of the KFU. KFU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5.2. Use of Classified and Proprietary Information

- 5.2.1. All information and systems owners must classify the information assets on their custody and responsibility by taking necessary assistance from the Quality Management Office of the Deanship of Information Technology (KFU/DIT/QMO). KFU information that are contained on core platform/ website/ portals/ internet/ intranet / extranet related systems should be classified as either confidential or not confidential; private, for internal use, or public; critical or sensitive or not critical; and so on.

Examples of confidential information include but are not limited to: university and its allied partnership company private, university strategies, government sensitive, competitor sensitive, trade or research secrets, specifications, students and faculty lists and research data.

5.2.2. All information owners and employees should take all necessary steps to prevent unauthorised access to the information assets on their custody. All owners of the information assets must ensure that all engineers, technicians, professionals, operators and administrators as well as the authorised users must get an understanding of the university's need and its internal control procedures so that they can plan their maintenance or change process, if any.

5.2.3. All the professionals and authorised owners of the classified information assets must exercise due professional care in performing their maintenance and auditing tasks.

5.2.4. All major and critical changes to information assets must be adequately planned and all assistants to the creating and changing processes must be properly supervised.

5.2.5. All the administrators and accountable owners of the information assets must consider whether their reports and statements are prepared using the appropriate techniques and templates using the industry standard best practices in general (such as ISO27001) and the manufacturers standards in specific as the same shall be obtained from the manufacturers at the time of acquisition of the product.

5.2.6. The following are certain implementation guidelines for protecting the information assets:

a) It is prohibited to disclose or higher to persons not employed by the KFU, any information classified as 'INTERNAL USE', unless this has been authorised by the information owner. Such information includes, but not limited to:

Policies and procedures; System architecture; Application information; Network diagrams; Hardware and software technical specifications; Information related to projects past or current; Information related to copyrighted materials; etc.

b) All data classified as "FOR INTERNAL USE" or higher should not leave the KFU premises without prior approval by the information owners.

They must be stored in a locked cabinet or storage area. Access to the area must be controlled.

- c) If any information stored in electronic form that is no longer needed and is classified as "INTERNAL USE" and above must be destroyed in a secure way, using approved equipment and procedures, so that data cannot be recovered.
- d) All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (Ctrl + Alt + Del key combination for the Windows users) when the host will be unattended.
- e) The use of storage media and peripheral devices (e.g. DVD writers, USB ports, flash disks etc.) must be limited (to the maximum extent possible) so as to cover business needs only. Employees must only use the storage media (e.g. floppy disks, USB disks etc.) provided by KFU or by its authorised service provider.
- f) Storing information of different classification levels in the same storage media must be avoided. Media must be protected according to the classification level of the information that they contain.
- g) Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system (Kensington locks).
- h) Posting by email user from the KFU email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of KFU, unless posting is in the course of authorised service duties.
- i) All hosts used by the user that are connected to the KFU Internet / Intranet / Extranet, whether owned by the user or KFU, shall be continually executing approved virus-scanning and cleaning software


with a current virus database unless overridden by departmental or group policy.

- j) All users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

5.3. Use of Information classified as “CONFIDENTIAL” or above

The following rule(s) shall be applied for any kind of materials (e.g. presentation materials, technical documents etc.) that contains information classified as “CONFIDENTIAL ”and/or above.

5.3.1. When the delivery of confidential information to a third party is required, the following rules shall apply:

- a) The information owner must authorize it in writing.
- b) A Non-Disclosure Agreement must be signed by the third party before receiving the material. ( ***please refer to section 6.1.5 Confidentiality Agreements*** of the ISP manual).
- c) When employees themselves need to carry such documents, they must deliver them only to the designated recipient.
- d) Such information must never be left unattended on office desks.

5.3.2. When receiving of confidential information from a third party is required, the following rules shall apply:

- a) Confidential documents must only be accepted by authorized employees.
- b) A formal written confirmation of receipt at the time when the document comes into their possession must be provided or a sign-off on the appropriate delivery document, of which a copy is obtained, can be made.

5.3.3. All such kind of confidential materials (e.g. Documents and Data on Medias) must be kept in a fireproof area. The Information Owner must be immediately informed should such information be lost,

disclosed to unauthorised persons, or there is suspicion of any of the above. The Information Security Incident Handling Procedure must be triggered.

5.3.4. Making additional copies using any method (e.g. photocopies) of confidential information must not take place without the permission of the Information Owner.

5.3.5. The employee must be present at the printer or copier when confidential information is being printed or copied. The employee must make sure that all printouts are immediately removed from the device so that they are not revealed to unauthorised persons.

5.3.6. Use of encryption of confidential data stored on electronic devices must be considered. All data classified as "CONFIDENTIAL" or higher, that is transferred through un-trusted networks (e.g. Internet) or semi-trusted networks and whenever there is a strong need for the protection of their confidentiality and integrity, must be encrypted prior to their transmission

5.3.7. Conversations or chatting in public places or open offices that refer to classified "CONFIDENTIAL" and above information, must be performed with caution so that unauthorised disclosure to third parties is avoided.

5.4. Unacceptable Use

The following activities are, in general, prohibited. KFU employees and/or contractors may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

The lists below are by no means exhaustive, but attempt to provide a framework for systems and network related activities which fall into the category of unacceptable use and, therefore, strictly prohibited, with no exceptions include, but not limited to:

- 5.4.1. Under no circumstances is a user of the KFU network authorized to engage in any activity that is illegal under local, state, Saudi Arabian or International law while utilizing KFU owned resources.
- 5.4.2. The KFU reserves the right to decide what is considered extensive (and thus not acceptable) personal use. Users are not allowed to play games on the KFU information systems.
- 5.4.3. It is stressed that personal use of the KFU information systems is a privilege and not a right. Abuse of this privilege may result in its revocation and / or disciplinary and legal action.
- 5.4.4. Use of data and software originating from untrusted sources are prohibited. Unauthorized software must not be used, installed or stored in information systems. There is a serious risk that the software could be infected with malicious software, which may harm information and information systems.
- 5.4.5. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by KFU, are prohibited.
- 5.4.6. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which KFU or the end user does not have an active license is strictly prohibited.
- 5.4.7. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- 5.4.8. Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.

5.4.9. Using a KFU computing asset to activity engaged in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction is prohibited.

5.4.10. Other prohibited activities includes, but not limited to:

- a) Making fraudulent offers of products, items, or services originating from any KFU account; and making statements about warranty, expressly or implied, unless it is a part of normal job duties; are prohibited.
- b) Effecting security breaches or disruptions of network communication.
- c) Port scanning or security scanning is expressly prohibited unless prior notification to Information Security responsible (KFU/DIT/QMO) is made.
- d) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- e) Circumventing user authentication or security of any host, network or account.
- f) Interfering with or denying service to any user other than the employee's host (e.g. Denial of service attack).
- g) Users are not allowed to use, within the KFU premises, information systems and equipment not belonging or provided by the KFU or its approved service provider.
- h) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- i) Providing information about, or lists of, KFU employees, faculty, students to parties outside KFU, unless it is authorised for valid reason by a competent authority of the KFU.
- j) Direct Access to systems of the network via dial-in modems is not allowed, with the exception of special occasions where the Owner of the system or service requests so, and the Dean of Information Technology has approved the request.

5.5. Limited Personal Use of Information & Communication Systems

5.5.1. Personal use of corporate information systems is allowed only within the limits defined by KFU. Information systems are provided to KFU community as a tool to perform business activities and/or retrieve study and research materials relevant to their course and should be used for that reason. **Occasional use of information systems for personal purposes is allowed only when:**

- a) It will not result in loss of any kind to KFU (or the operational cost to the KFU is insignificant).
- b) Such use does not aim in personal benefit for the user or for any business entity other than the KFU (personal business activities of the employee e.g. family businesses, businesses the user is affiliated with either for profit or not, etc.).
- c) It does not consume considerable systems resources.
- d) It does not affect employee productivity.
- e) Does not disturb colleagues, causing conflicts.
- f) Does not disturb any activity of the university.
- g) Does not serve political interests.
- h) Does not perform malicious or illegal activities.
- i) Does not contravene this or any other university and government policy.

5.5.2. User accounts (User-IDs) to access KFU Internet Services (including e-mail services) are strictly personal. Users with access to these services must use the accounts in a responsible way. They must access Internet / e-mail using only their personal account and must not allow others to make use of their account. The legitimate user is accountable for any inappropriate and illegal use of the Internet and e-mail made through his account.

5.5.3. **The telephony system of the KFU must be used mainly for business purposes. Personal use is allowed only if the following are met:**

- A. It does not reduce their productivity or discomforts other employees
- B. the business activities of the KFU are not affected


- C. the operational cost is negligible
- D. the system is not used for illegal or malicious purposes

5.6. Communication via Internet, E-mail, and Blogging

5.6.1. **Email and other type of communication activities that are strictly prohibited, with no exceptions include, but not limited to:**

- a) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- b) Sending large numbers of personal messages or being on-line on the Internet for extended periods of time, especially during working hours. Personal Blogging and/or Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- c) Sending extensive personal messages (which require significant amount of time for composing or reading).
- d) Sending personal messages with large attachments.
- e) Bulk sending of messages
- f) Extensive browsing or blogging on the Internet
- g) Any form of harassment via email, telephone or SMS, whether through language, frequency, images, music, voice, or size of messages.
- h) Unauthorized use, or forging, of email header information.
- i) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- j) Use of unsolicited email originating from within KFU's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by KFU or connected KFU's network.
- k) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.6.2. Masquerading or attempting to masquerade a user identity (sender identity) via the e-mail and Internet services is strictly prohibited. The user name, the e-mail address, the role within the KFU and other relevant information contained in e-mail messages and postings must depict the actual sender.

- 5.6.3. E-mail messages must not be deleted, unless they have been archived first, where necessary. Employees must periodically delete e-mail messages that are no longer required for business purposes.
- 5.6.4. Blogging by employees, whether using KFU's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of KFU's systems to engage in blogging or browsing is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate KFU's policy, is not detrimental to KFU's best interests, and does not interfere with an employee's regular work duties. Blogging from KFU's systems is also subject to monitoring.
- 5.6.5. KFU's Information Security Framework and Policies, especially the confidentiality requirements, also applies to blogging and personal email messages.  **please refer to section 5.2: Use of Classified and Proprietary Information & section 5.3: Use of Information classified as "CONFIDENTIAL" or above** of this policy for details. Subsequently, sending information via the Internet and e-mail is not allowed for information classified as "CONFIDENTIAL" and above, unless authorization is granted and adequate security mechanisms are implemented.
- 5.6.6. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of KFU and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by KFU's or Ministry of Higher Education's policies on ethics and social conducts.
- 5.6.7. Users must act in a way that enhances the image of the KFU does not harm its interests in any way. It must be stressed that an e-mail message sent by an employee to a student, supplier and generally to a third party, has the exact same impact with any other communications means in terms of how the client perceives the communication with the KFU.

- 5.6.8. Users must not make agreements or negotiations over the Internet that may commit the KFU in any way, without possessing the appropriate credentials (Authority / Right of Signature).
- 5.6.9. Before an employee executes a transaction via the Internet (e.g. makes an agreement or places an order) on behalf of KFU, the identity of the parties involved must be confirmed. Ideally, Digital Signatures and/or Digital Certificates must be used for this purpose. If this is not feasible, other channels must be used (e.g. Fax, mail).
- 5.6.10. Users wanting to communicate with external third parties (clients, suppliers, etc.) must exclusively use the KFU e-mail system and their assigned e-mail address.
- 5.6.11. Users must not send, receive or forward information using non-corporate e-mail addresses, such as Hotmail, Yahoo, etc. Even in cases where employees need to send a business message while being away of the KFU premises and not having Web mail access, they must not use other e-mail systems.

5.7. Installation and modification of Software and Electronic Equipment

- 5.7.1. Installation and modification (e.g. of the security or network configuration) of software or electronic equipment of KFU information systems (desktop computers, laptop computers, special purpose terminals etc.) is prohibited. Any installation or modification to the systems must be performed only with the approval of the Deanship / Department Manager to which the information belongs to, and with the permission of the relevant IT Systems & Network Management department (to achieve architectural compatibility and to ensure only authorised software is used). Modifications must be performed only by the employees or contracted professional authorised by Deanship of Information Technology of KFU (KFU/DIT).

5.7.2.Modification, installation and any type of alteration to the baseline architecture will be subject to the Change Management and/or Configuration Management procedures as specified by the (KFU/DIT).

5.7.3.Any intentional action, that may have negative effect on the proper and continuous operation of information systems, on the availability of systems to legitimate users or any other action that may be considered aggressive or offensive by third parties, is strictly prohibited.

5.8. Accessing Files of other Users, Unauthorized access attempts & Disk Sharing

5.8.1.Users should not read, modify, delete or copy files that belong to another user without asking for permission from the file Owner first. Having the capability to read, modify, delete or copy files belonging to other users does not imply having the right to do so, unless this right has been explicitly granted.

5.8.2.Users are not allowed to attempt gaining unauthorised access to any of the KFU or third party information systems, or to harm, modify or prevent their operation.

5.8.3.Users are not allowed to intercept, or by any other means acquire, passwords, cryptographic keys or any other access control mechanism, which would facilitate unauthorised access to the KFU's or third party information systems.

5.8.4.Any attempt to bypass access control and protection mechanisms implemented in information systems is prohibited.

5.8.5.Employees are prohibited from connecting any device (personal computer, laptop, network equipment etc.) to the corporate network, or allow others to use their connection (i.e. their LAN cable), without permission from the Network Owner.

5.8.6.Users must not create disk shares on their personal computers. When there is a business need to share data, centralized infrastructures must be used (e.g. file servers), under the supervision of the System Administrator and/or the Security coordinator of the Deanship of Information Technology. Creation of disk shares on any other type of

servers (application servers, database servers) apart from file servers should be avoided. All requests for centralized file sharing or a space on the centralized server must be sent to the Deanship of Information Technology through the workflow tool provided for help-desk (i.e. Remedy System).

5.9. Encryption Keys & Passwords

- 5.9.1. Keep passwords secure and do not share accounts. Revealing user's account password to others or allowing use of his / her account by others is prohibited. This includes family and other household members when work is being done at home. All users are responsible for the security of their passwords and accounts.
- 5.9.2. All users authorized to use encryption for specific purposes, must disclose the decryption keys to the Chief Information Security Manager (CISM) within the deanship of Information Technology, whenever this is requested for business reasons.
- 5.9.3. System level (root access or master key passwords) passwords should be changed quarterly and must be written inside a sealed envelope to be stored in safe under the custody of the data centre manager. All other user level passwords should be changed every six months.
- 5.9.4. The loss or disclosure of secret keys or private keys must be treated as a security incident and be immediately reported.
- 5.9.5. Users must under no circumstances use the same password for both systems belonging to External Networks (e.g. the Internet) and for KFU internal systems.
- 5.9.6. Passwords must never be written or stored in places accessible to others (e.g. on a piece of paper under the keyboard). The user is responsible for protecting his passwords and never revealing them to others.

5.9.7. All passwords of an information system must be changed immediately if there is the suspicion or proof that passwords have been revealed to unauthorized users.

5.9.8. Passwords must bear the following security characteristics:

- a) They must be at least eight (8) characters long
- b) They must be hard to find or guess. More specifically, they must not consist of main words, of username derivatives, of place-names, of acronyms and common character sequences (e.g. "123456"). Additionally, passwords must not consist of personal data such as family names, car plate numbers, birth dates or anniversaries and constant parts changed in a predictable way (e.g. using password "X11JAN" for January followed by "X11FEB" on February).
- c) They must contain at least one character from three character sets as a minimum: uppercase, lowercase, numbers and symbols.
- d) They cannot use more than four (4) consecutive characters of same character type (uppercase, lowercase, numbers and symbols).
- e) Password change must be enforced (by the operating system or the application) at least every sixty (60) days. The new passwords must not be the same with the previous five (5) ones (password history). They also must differ from previous ones on at least half of the characters.

5.9.9. To avoid launching successful attacks to multiple systems, simple and privileged users must use separate passwords for every one of the critical information systems they have access to.

5.10. Mobile computing / Teleworking and Using them in Public places

5.10.1. Carrying mobile computing and/or teleworking equipment out of KFU premises is prohibited without prior approval accompanied by a written authorisation. If there is such a requirement, sensitive information stored on mobile computer must always be encrypted using approved methods and cryptographic technologies.

5.10.2. Mobile computing / teleworking equipment must be returned to relevant managers, after conducting the specific activities or cease to be employed. Any loss of mobile computing / teleworking equipment must be immediately reported to the user's supervisor.

5.10.3. Connection to un-trusted networks should be avoided when there is no business need. When a mobile computer is connected to external networks, and especially if it is connected to un-trusted networks (e.g. Internet), all necessary protection mechanisms at network level (e.g. personal firewalls, antivirus software etc.) must be activated.

5.10.4. When using mobile computers in public places the risk of sensitive information being disclosed to third parties is high (e.g. shoulder surfing). Therefore, the use of such equipment in public places or, in any case, off-site must be done with special caution. **The users must abide by the following:**

- a) Be very careful when entering their password.
- b) Terminate any unnecessary connections.
- c) Lock their computers or shutdown the system when they have completed their tasks.
- d) Secure their laptops using appropriate physical protection mechanisms e.g. locked drawers' special locks (Kensington locks).

5.10.5. All the mobile storage media (e.g. floppy disks, CDs, memory sticks, etc.) must be checked for malicious software before use.

5.11. Incident and Weakness Reporting


5.11.1. All users must report any weaknesses they may detect to IT systems or of any other nature that compromises KFU security. By no means should they try to exploit the detected weakness and should only reveal it to authorised parties.

5.11.2. Users are not allowed to try and solve the problem themselves. Problems must be solved with the assistance of the Help Desk and/or IT Technical Support Department.

5.11.3. All users are obliged to report to the Help Desk (through Remedy System) any problem identified regarding an information system. All staff must remain alert to security incidents. When a security incident is suspected or confirmed, it must be reported to the Help Desk as soon

as possible. The user must convey all information related to the incident e.g. the symptoms of the problem, possible messages that appear, etc.

6. Disciplinary Actions and KFU Rights

 ***please refer to Chapter 16 Disciplinary Actions and KFU Rights*** of the Information Security Framework and Policy Manual.