ACCESS CONTROL POLICY

KING SAUD UNIVERSITY
DEANSHIP OF eTRANSACTIONS & COMMUNICATION

VERSION 1.1
INTERNAL USE ONLY
## Revision History

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Date of Revision</th>
<th>Ver.</th>
<th>Validity</th>
<th>Description of change</th>
<th>Reviewed By</th>
<th>Approved By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>18/03/12</td>
<td>1.0</td>
<td>One Year</td>
<td>Initialization</td>
<td>Nasser A. Ammar</td>
<td>Dr. Mohammed A Alnuem</td>
</tr>
<tr>
<td>2</td>
<td>02/03/13</td>
<td>1.1</td>
<td>One Year</td>
<td>Department Ownership Changed</td>
<td>Mr. Toqeer Ahmad</td>
<td>Mr. Mohammed A Alsarkhi</td>
</tr>
<tr>
<td>3</td>
<td>04/03/13</td>
<td>1.1</td>
<td>One Year</td>
<td>No Change</td>
<td>Mr. Toqeer Ahmad</td>
<td>Mr. Mohammed A Alsarkhi</td>
</tr>
</tbody>
</table>

### Distribution List

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Version Number</th>
<th>Name</th>
<th>Designation</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# ACCESS CONTROL POLICY

## TABLE OF CONTENTS

1. **PURPOSE** ........................................................................................................... 5
2. **SCOPE** ............................................................................................................. 5
3. **POLICY ENFORCEMENT / COMPLIANCE** ......................................................... 5
4. **WAIVER CRITERIA** .......................................................................................... 5
5. **RELATED POLICIES** ....................................................................................... 6
6. **DOCUMENT OWNER** ....................................................................................... 6
7. **POLICY MANAGEMENT** .................................................................................. 6
8. **POLICY STATEMENT** ....................................................................................... 7
   8.1. **INFORMATION ACCESS BUSINESS REQUIREMENTS** .............................. 7
   8.2. **USER ACCOUNT MANAGEMENT** ............................................................... 7
   8.3. **ACCESS AUTHORIZATION AND PRIVILEGE** ......................................... 8
   8.4. **USER PASSWORD MANAGEMENT** ........................................................... 8
   8.5. **USER ACCESS RIGHTS REVIEW** .............................................................. 9
   8.6. **PASSWORD CONTROL** ............................................................................ 9
   8.7. **UNATTENDED USER EQUIPMENT PROTECTION** .................................... 9
   8.8. **CLEAR DESK AND CLEAR SCREEN SECURITY** ...................................... 9
   8.9. **NETWORK RESOURCES** ....................................................................... 10
   8.10. **REMOTE USER ACCESS AUTHENTICATION** .......................................... 10
   8.11. **NETWORK EQUIPMENT ACCESS AUTHENTICATION** ......................... 10
   8.12. **REMOTE ACCESS MAINTENANCE PROTECTION** .................................... 11
8.13. NETWORK SEGMENTATION ................................................................. 11
8.14. NETWORK CONNECTIONS CONTROL ............................................. 11
8.15. INFORMATION FLOWS CONTROL ..................................................... 11
8.16. SECURE LOG-ON OF OPERATING SYSTEMS ..................................... 12
8.17. USER IDENTIFICATION AND AUTHENTICATION ................................. 12
8.18. UTILITY PROGRAMS CONTROL ......................................................... 12
8.19. SESSION TIME-OUT CONTROL ......................................................... 13
8.20. CONNECTION TIME CONTROL ......................................................... 13
8.21. APPLICATION SYSTEMS ACCESS CONTROL ..................................... 13
8.22. SENSITIVE APPLICATION SYSTEMS SEPARATION ........................... 13
8.23. TELEWORKING ACTIVITIES CONTROL ........................................... 13

9. GLOSSARY ........................................................................................ 15
1. PURPOSE
The Access Control Policy aims to manage logical and physical access only to authorized individuals and devices inside the King Saud University eTransactions & Communication Deanship premises.

2. SCOPE
This policy applies to King Saud University (KSU) – eTransactions & Communication (ETC) Deanship and all parties, its affiliated partners or subsidiaries, including data processing and process control systems, that are in possession of or using information and/or facilities owned by KSU-ETC Deanship.

This policy applies to all staff/ users that are directly or indirectly employed by KSU-ETC Deanship, subsidiaries or any entity conducting work on behalf of KSU that involves the use of information assets owned by ETC Deanship.

3. POLICY ENFORCEMENT / COMPLIANCE
Compliance with this policy is mandatory and ETC Deanship managers shall ensure continuous compliance monitoring within their departments. Compliance with the statements of this policy is a matter of periodic review by Risk & Information Security Department. Any violation will result in disciplinary action by ISMS Steering Committee.

Disciplinary action will be depending on the severity of the violation which will be determined by the investigations. Actions such as termination or others as deemed appropriate by ETC Management and Human Resources Department shall be taken.

4. WAIVER CRITERIA
This policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the ISMS Steering Committee, including justification and benefits attributed to the waiver.

The policy waiver period have maximum period of one year, and shall be reassessed and re-approved, if necessary for maximum three consecutive terms. No policy shall be provided waiver for more than three consecutive terms.
5. RELATED POLICIES

- Compliance Policy.
- Information Security Policy.
- Communications and Operations Management Policy.
- Physical and Environmental Security Policy.

6. DOCUMENT OWNER

- ISMS Manager.

7. POLICY MANAGEMENT

Technological advances and changes in the business requirements will necessitate periodic revisions to policies. Therefore, this policy may be updated to reflect changes or define new or improved requirements.

Deficiencies within this policy shall be immediately communicated to the Information Security Officer. Policy changes will require the approval of the ISMS Steering Committee and Risk & Information Security Department.

Change log shall be kept current and will be updated as soon as any change has been made.
8. **Policy Statement**

KSU ETC Deanship access control rules and rights for each user or group of users shall be clearly stated. Both types of access controls logical and physical shall be considered together for optimum security implementation.

8.1. **Information Access Business Requirements**

8.1.1. Access to information shall be controlled on the basis of business and security requirements and the access control rules defined for each information system. These rules shall consider the following:

- Security requirements of the business application(s);
- An identified business requirement for the user to have access to the information or business process (‘need to know’ principle);
- All access is denied unless specifically approved under the provisions of this policy;
- Legal and/or contractual obligation to restrict and protect access to information systems.

8.1.2. Access for contractors, consultants or third party personnel to KSU ETC Deanship’s business information assets shall be provided only on the basis of a contractual agreement. This agreement shall include, but not limited to:

- The terms and conditions for access provided;
- The security responsibilities of the contractors, consultants or vendor personnel;
- Agreement by the contractors, consultants or third party personnel to abide to KSU ETC Deanship’s information security policies.

8.2. **User Account Management**

8.2.1. KSU ETC Deanship shall define a formal access control procedure that includes clear steps in relation to requesting, creating, modification, suspending and revoking user accounts.

8.2.2. The granting of user access, changes to existing user access rights and removal of user access shall be authorized by the asset owner taking into account the following:

- Least privilege (‘need to know’ principle);
- Segregation of duties;
- Level of access required.

8.2.3. All users of shall be identified with a unique credential that establishes identity. User credentials shall require at least one factor of authentication (e.g. password, token number or biometric devices).
8.3. **ACCESS AUTHORIZATION AND PRIVILEGE**

8.3.1. All authorized user accessing ETC Deanship information assets shall be defined and documented. Authorizations process shall be tracked and logged as follow:

- Date of authorization;
- Identification of individual approving access;
- Description of access privileges granted;
- Description of why access privileges granted.

8.3.2. Segregation of duties and least privileges principles shall be followed when granting access privileges to KSU ETC Deanship department users.

8.4. **USER PASSWORD MANAGEMENT**

8.4.1. Passwords shall be immediately changed if there is any suspicion of password compromise; and this shall be reported immediately Customer Care Helpdesk.

8.4.2. Individual ETC Deanship department shall be responsible for changing all information system default usernames and passwords before any of their information system is put into operation.

8.4.3. Users and administrators shall follow the following security characteristics when selecting passwords:

- Password shall be minimum of 8 characters length;
- Password shall be combination of:
  - At least one uppercase alphabetic character (A-Z);
  - At least one lowercase alphabetic character (a-z);
  - At least one special character (e.g. @, %, &);
  - At least one number (0-9).
- Password shall not based on personal information, names of family, etc;
- Password shall not be guessable or a word found in a dictionary;
- Blank password shall not be allowed;
- Users shall be required to change their password immediately after their first login to any system;
- User account shall be locked after 3 unsuccessful attempts;
- Password change shall be enforced (by the operating system or the application) at least every 42 days. The new passwords shall not be the same with the previous 8 ones (password history);
- Initial password shall be only used one time;
- Password shall be stored and transmitted in protected (e.g. encrypted or hashed) form.
8.5. **User Access Rights Review**

8.5.1. Asset Owners in cooperation with Information Security Officer and related departments (i.e. ICT Infrastructure Department units, Data Centre, Applications) shall review user access rights and privileges at least once a year.

8.5.2. Upon detection of any misconduct of privileged access rights, the Information Security Officer shall recommend to department manager to restrict such privileges.

8.6. **Password Control**

8.6.1. Users shall not insert password into email messages or electronic communications.

8.6.2. Users shall not distribute their username and password to other users; thus users shall be accountable for any activity associated with their access rights.

8.6.3. Users shall not capture or otherwise obtain passwords, decryption keys, or any other access control mechanism, which could permit unauthorized access.

8.7. **Unattended User Equipment Protection**

8.7.1. Screen saver password shall be enabled on all information assets (e.g. desktop, laptops and servers) to prevent unauthorized access. The screen saver timer shall be set to 10 minutes of inactivity or less.

8.7.2. Each user shall terminate active sessions when activities are finished.

8.7.3. Each user shall lock his equipment before leaving his desk.

8.8. **Clear Desk and Clear Screen Security**

8.8.1. At a minimum, the following guidelines shall be followed and implemented by all users to promote ETC Deanship's clear desk and clear screen policy:

- Paper and information media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside normal working hours;
- Sensitive or critical business documentation shall be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated;
- Personal computers, computer terminals and printers shall not be left logged on when unattended; and shall be protected by password protected screen savers;
- Photocopiers and faxes shall be locked (or protected from unauthorized use in some other way) outside normal working hours;
- Sensitive information, when printed, shall be immediately cleared from printers.
8.8.2. The ISMS Manager shall communicate the clear desk and clear screen policy to the employees in their own areas; and shall periodically monitor their activities to ensure users compliance.

8.8.3. Information Security Officer shall ensure that proper awareness training addresses clear desk and clear screen policy is delivered to all ETC Deanship employees, contractors, consultants and any external parties.

8.9. **NETWORK RESOURCES**

8.9.1. Access to networks and network services shall be authorized and controlled on the basis of business, security requirements and access control rules defined for each network. These rules shall take into account the following:

- Security requirements of the network or network service(s);
- An identified business requirement for the user to have access to the network or network service (‘need-to-have’ principle);
- The user’s security classification and the security classification of the network;
- Legal and/or contractual obligation to restrict or protect access to information assets.

8.10. **REMOTE USER ACCESS AUTHENTICATION**

8.10.1. Remote user access to ETC Deanship's networks shall be restricted to authorized users only and shall follow the appropriate user authentication methods.

8.11. **NETWORK EQUIPMENT ACCESS AUTHENTICATION**

8.11.1. As part of an overall asset register, ICT Infrastructure Department shall identify all network equipment by individual names; and shall maintain a record of all network equipment along with location and purpose of the equipment.

8.11.2. Network diagrams shall contain, but not limited to:

- All network equipment along with their IP Addresses;
- All communication links (primary and stand-by) along with their bandwidths and data type for which the line is used for (voice / data);
- Adequate version control mechanism.

8.11.3. An updated network diagram shall be maintained. ICT Infrastructure Department shall conduct periodic reviews to ensure that the diagram is updated to reflect the existing network architecture. Network diagrams shall be updated when there are changes made to the network architecture.

8.12.1. The use of network diagnostic and security tools shall be limited to specifically designated staff, and in accordance with their job responsibilities.

8.12.2. Any remote administration connections authorized by KSU shall use strong authentication (such as two-factor authentication) as well as corresponding encryption methods (such as SSH, SSL and VPN).

8.13. **Network Segmentation**

8.13.1. KSU-ICT Infrastructure Department information systems network shall be divided into logical segments or domains based on the following criteria, but not limited to:

- Access requirements (e.g. Users, IT, Management);
- Relative cost and performance impact of incorporating suitable technology;
- Value and classification of information stored or processed in the network (e.g. Critical, Sensitive);
- Levels of trust (e.g. Trusted, Internet, DMZ);
- Lines of business (e.g. Service, Support).

8.13.2. Internal network shall be segregated from the external network with different perimeter security controls on each of the networks.

8.14. **Network Connections Control**

8.14.1. The connection capability of users shall be restricted through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions may include, but not limited to:

- Messaging (e.g. electronic mail);
- File transfer;
- Interactive access;
- Application access.

8.15. **Information Flows Control**

8.15.1. All routing traffic shall be authorized by ICT Infrastructure Department based on business communications requirements and in coordination with business process owners.

8.15.2. ICT Infrastructure Department shall implement appropriate routing control mechanisms to restrict information flows to designated network paths.
8.15.3. KSU-ICT Infrastructure Department shall ensure proper management and technical oversight are performed over security perimeter structure (e.g. firewall) and current configuration. The following shall be covered, but not limited to:

- Documenting the security perimeter rules and reviewing them in a regular basis;
- Documenting configuration changes and getting management approval;
- Getting management approval prior applying any changes to security perimeter rules;
- Taking an adequate care while applying changes on the security perimeter rules to ensure minimal distortion to KSU-ETC Deanship environment.

8.16. **Secure Log-on of Operating Systems**

8.16.1. System shall limit the number of unsuccessful logon attempts allowed; the following shall be considered:

- Recording both successful and unsuccessful attempts;
- Forcing a time delay before further logon attempts are allowed or rejecting any further attempts without specific authorization;
- Disconnecting data link connections;
- Sending an alarm message to the system console if the maximum number of logon attempts is reached.

8.16.2. System administrators shall review all unsuccessful log attempts in a periodically basis.

8.16.3. System shall display a general notice warning that the computer shall only be accessed by authorized users.

- The logon process on any system shall display only the limited information about the system and its purposed use.

8.17. **User Identification and Authentication**

8.17.1. System shall validate the log-on information only upon completion of all input data. If an error condition appears, the system shall not indicate which part of the data is correct or incorrect.

8.17.2. Messaging & Identity Management Department shall identify and authenticate all users uniquely before granting them the appropriate network/system access.

8.18. **Utility Programs Control**

8.18.1. Access to and use of system programs shall be restricted and controlled.

8.18.2. All unnecessary system utilities and software shall be removed.
8.19. **Session Time-out Control**
8.19.1. During the logon procedure, system shall limit the maximum and minimum time allowed. If exceeded, the logon shall be terminated.

8.20. **Connection Time Control**
8.20.1. Wherever possible, all critical information systems shall have a defined time window for access and connectivity.

8.21. **Application Systems Access Control**
8.21.1. Controls shall be defined to control outputs from application systems that handle sensitive information, and those outputs are only sent to authorized terminals and locations.

8.22. **Sensitive Application Systems Separation**
8.22.1. Physical and/or logical isolation for sensitive systems shall be defined.
8.22.2. Sensitive application that handles sensitive data shall run on a dedicated operating system, where possible.
8.22.3. When a sensitive application requires running on a shared environment, the application owner shall identify and accept associated risks of the shared resources.
8.22.4. Application shall be configured to run only limited services as required and justified by business needs.

8.23. **Teleworking Activities Control**
8.23.1. A formal management approval shall be obtained, and all appropriate security arrangements and controls shall be in place before teleworking activities are authorized.
8.23.2. Laptops and home personal computers shall not be used for business activities without explicit authorization from management.
8.23.3. When the teleworking activities are completed, revocation of authority, access rights, and the return of equipment shall be performed immediately.
8.23.4. An accurate and up to date record of all the teleworking activities shall be maintained.
8.23.5. KSU shall only authorize use of KSUETC Deanship’s owned devices for teleworking and remote connectivity to their network. The following security arrangements shall be considered by the Asset owner:

- Ensure physical security of devices and protection from theft / lost;
- Ensure the encryption of the devices;
- Use of appropriate anti-malware and devices security controls (e.g. antivirus and personal firewalls);
- Connect to KSU-ICT Infrastructure Department network using secure tunneling method (e.g. SSL, VPN);
- Proper authentication / authorization mechanisms are implemented;
- Backup all sensitive information.
### 9. Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Asset is anything that has value to the organization.</td>
</tr>
<tr>
<td>Asset Custodian</td>
<td>It is a person or department who has final responsibility of the asset.</td>
</tr>
<tr>
<td>Asset Owner</td>
<td>It is a person who is using the asset.</td>
</tr>
<tr>
<td>Availability</td>
<td>The property of being accessible and usable upon demand by an authorized entity.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.</td>
</tr>
<tr>
<td>Control</td>
<td>It is a means of managing risk, including policies, procedures, guidelines, etc., which can be of administrative, technical, management, or legal nature.</td>
</tr>
<tr>
<td>Guideline</td>
<td>A description that clarifies what should be done and how, to achieve the objectives set out in policies.</td>
</tr>
<tr>
<td>Incident</td>
<td>A vulnerability and threat together result in an incident.</td>
</tr>
<tr>
<td></td>
<td>An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.</td>
</tr>
<tr>
<td>Information Processing Facilities</td>
<td>Any information processing system, service or infrastructure, or the physical locations housing them.</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
<td>The preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Information Security Event</strong></td>
<td>An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.</td>
</tr>
<tr>
<td><strong>ISMS</strong></td>
<td>An Information Security Management System is a set of policies concerned with information security management.</td>
</tr>
<tr>
<td><strong>Mobile Code</strong></td>
<td>It is software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.</td>
</tr>
<tr>
<td><strong>Service-Level Agreement (SLA)</strong></td>
<td>It is a negotiated agreement between two parties where one is the customer and the other is the service provider.</td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td>A plan of action to guide decisions and actions. The term may apply to government, private sector organizations and groups, and individuals. The policy process includes the identification of different alternatives, such as programs or spending priorities, and choosing among them on the basis of the impact they will have.</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>Risk is combination of the probability of an event and its consequence.</td>
</tr>
<tr>
<td><strong>Risk Analysis</strong></td>
<td>A systematic use of information to identify sources and to estimate risk.</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>Risk Assessment is defined as the overall process of risk analysis and risk evaluation, where risk analysis is defined as the systematic approach to identify an organization’s exposure to uncertainty and to estimate the risk. Risk evaluation is the process of comparing the estimated risk against given risk criteria to determine the significance of risk.</td>
</tr>
<tr>
<td><strong>Risk Evaluation</strong></td>
<td>Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.</td>
</tr>
</tbody>
</table>
| **Risk Management** | Coordinated activities to direct and control an organization with regard to risk.  
**NOTE:** Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Treatment</strong></td>
<td>Process of selection and implementation of measures to modify risk.</td>
</tr>
<tr>
<td><strong>Third Party</strong></td>
<td>That person or body that is recognized as being independent of the parties involved, as concerns the issue in question.</td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>A threat has the potential to cause an unwanted incident which may result in harm to a system.</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>Vulnerability is defined as a weakness associated with an asset.</td>
</tr>
</tbody>
</table>