سياسة ضبط الدخول
Access Control Policy

Table of Contents

Issue Control

Change Approval	This document may be viewed, printed by authorized personnel only. Any changes to this policy shall be reviewed and accepted by the IT Deanship and approved by Information Security Manager.
Review and Update	A policy review shall be performed at least on an annual basis to ensure that the policy is current. It is the responsibility of the Information Security Manager to facilitate the review of this policy on a regular basis. Personnel and Department Head from Relevant Departments shall also participate in the annual review of this Policy.

Policy Structure

1. Purpose

Access control policy of KAU is to manage logical and physical access only to authorized individuals and devices inside the KAU premises.

2. Scope

This policy applies to KAU and all parties, its affiliated partners, companies or subsidiaries, including data processing and process control systems, that are in possession of or using information and/or facilities owned by KAU.

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

3. Role and Responsibilities

Based on KAU's Organizational Structure, the following is a list of roles and their associated responsibilities towards this policy.

سياسة ضبط الدخول
Access Control Policy

1. IT Dean Role

- Enforce security policies within KAU environment to protect critical business information assets and software.
- Ensure that security policies are compliant with KAU legal and contractual requirement.
- Approve the use of all information systems used to process, store, or print sensitive information.
- Approve the new or modifications of existing security policies.

2. IT Deanship Role

- Distribute information security documents so that those who need such documents have copies or can readily locate the documents via an intranet site.
- Ensure the protection of information/infrastructure systems, according to the technological mechanisms defined by the system / application design team.
- Perform system/application/network security monitoring.

3. Information Security Department Role

- Define and maintain the information security policies.
- Prepare and periodically updates information security manuals needed to advance information security at KAU.
- Implement appropriate controls to protect the confidentiality, integrity and authenticity of sensitive information.

4. User Role

- Adhere to security policies, guidelines and procedures pertaining to the protection of sensitive data.
- Report actual or suspected vulnerabilities in the confidentiality, integrity or availability of sensitive data to Information Security Manager
- Use the information only for the purpose intended by KAU.

4. Compliance

Compliance with this policy is mandatory and KAU division managers must ensure continuous compliance monitoring within their divisions. Compliance with the statements of this policy is a matter of periodic review by Information Security Manager and any violation of the policy will result in corrective action by the Information Security Committee with cooperation with relevant security entities. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets.
- Actions like Financial/monetary penalty, termination of the employee or downgrading from the existing position as deemed appropriate by IT Dean, Administration Department, and the Legal Division

5. Waiver Criteria

This policy is intended to address information security requirements. If needed, waivers could be formally submitted to the Information Security Department, including justification and benefits attributed to the waiver, and must be approved by KAU Information Security Steering Committee.

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

6. Related Policies

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

7. Owner

- Information Security Manager.

8. Policy Statement

KAU access control rules and rights for each user or group of users shall be clearly stated in an access control policy. Both types of access controls logical and physical shall be considered together for optimum security implementation.

1. Information Access

Policy Objective	Policy Statement
Control access to information [A.11.1]	➢ Access to information shall be controlled on the basis of business and security requirements, as well as the access control rules defined for each information system. These rules shall take into account 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 or protect access to information systems. • Definition of user access profiles and management of user access rights throughout KAU's IT infrastructure. ➢ Access for contractors, consultants, or vendor personnel to KAU's critical business information assets shall be provided only on the basis of a contractual agreement. This agreement will provide: • The terms and conditions under which access is provided. • The responsibilities of the contractors, consultants or vendor personnel. • Agreement by the contractors, consultants or vendor personnel to abide KAU's Information Security Policy and Supplementary Information Security Policies. ➢ Access Control shall be implemented by defining group profiles with specific access privileges. Individual users shall not be assigned specific access but they will be provided access by means of membership into pre-defined user groups. ➢ Access to information assets shall be immediately revoked upon role change, resignation or termination of service.

2. Access Management

Policy Objective	Policy Statement
Ensure authorized user access and prevent unauthorized access to information systems [A.11.2]	➢ User access registration and procedures shall properly be documented and implemented. ➢ A formal user registration procedure shall be completed prior granting any access to KAU resources. ➢ All users shall be identified by unique identifier (e.g. UID, User ID); and authorized access to KAU assets by the asset owner or IT Dean. ➢ Users shall not distribute their username and password to other users; thus they will be accountable for any activity associated with their access rights. ➢ KAU shall ensure that redundant user IDs are not re-originated to

سياسة ضبط الدخول
Access Control Policy

Policy Objective	Policy Statement
	other users. ➢ Access to information assets required by third party staff shall be granted after the authorization, proper justification, access duration identification, and all the necessary information by the department director. ➢ For contract employees, consultants and all other third party personnel, access shall have an automatic expiry date not later than the conclusion of the contracted project. ➢ Detailed audit trails of user account creation, deletion and revocation of access rights must be recorded and kept for a minimum of 5 years. ➢ Information Security Department shall take additional precautions and introduce appropriate controls (e.g. security awareness) to prevent identity theft and the interception of user credentials by means of hacking, interception or social engineering techniques. ➢ All high privileges (e.g. administrator or root accounts) shall be assigned through a formal authorization process. All privileges shall be assigned only after the completion of the relevant authorization process. ➢ Segregation of duties shall be followed when granting access privileges to employees. ➢ Asset owners shall have the authority to grant allocation of privileges to the user. ➢ All user access privileges shall be reviewed by the asset owner every 6 months. ➢ All special privileged access rights such as administrator shall be reviewed and checked at regular intervals 3 months. ➢ Information Security Manager shall perform regular system audits to discover unused accounts; and subsequently shall be disabled and removed. ➢ Upon detection of any misconduct of privileged access rights, Information Security Department shall restrict such privileges and notify the asset owner and the Internal Audit Department for further action. ➢ Username and passwords shall be strictly kept private and confidential, communicated, used and distributed in a secure manner. ➢ Default usernames and passwords should be changed when new systems are acquired, before connecting it to KAU's infrastructure and placing it in production environment. ➢ Information Security Manager shall maintain complete history and documentation of system username and password changes and their assignments to personnel. ➢ Username and password assignment to employees and any changes shall be logged in an accurate up-to-date history log. ➢ Username locking and password expiry shall be defined based on the system requirements, asset classification, criticality of the system, and repercussions of compromise. ➢ The following rules shall be considered by all KAU employees as the

Policy Objective	Policy Statement
	baseline for selecting there passwords: • Password shall be a minimum of 8 characters length. • Password shall be combination of alphanumeric characters (both upper and lower case characters) and numbers. • Password shall not contain all or part of the username. • Password shall not be guessable or a word found in a dictionary (English or foreign). • Blank password shall not be allowed. • Users shall be required to change their password immediately after their first login to any system. • Password shall be changed every 30 days. • User account shall be disabled after three unsuccessful attempts. • Password shall be stored and transmitted in protected (e.g. encrypted or hashed) form. • Initial password shall be only used one time. ➢ Passwords shall be immediately changed if there is any suspicion of password compromise and reported immediately to department manager. ➢ All system shall not display the password being entered or consider hiding the password characters by symbols. ➢ Password files shall be stored in a secure place and encrypted if possible. ➢ All users shall read and sign KAU Non-Disclosure Agreements (NDAs) prior being provided with any access rights. ➢ KAU shall ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access.

3. User Responsibilities

Policy Objective	Policy Statement
Prevent unauthorized user access, and compromise or theft of information and information processing [A.11.3]	➢ Screen saver password shall be enabled by users on their own desktop, laptops and servers to prevent unauthorized access. The screen saver timer shall be set to 10 minutes of inactivity or less. ➢ Each user shall terminate active sessions when activities are finished. ➢ Awareness training to users shall cover all their necessary and expected actions; also it shall cover their responsibility toward the assets (clear desk and clear screen policies). ➢ Clear screen policy shall be followed by all employees for papers, removable media and information processing facilities in order to reduce the risks of unauthorized access, loss of and/or damage to

Policy Objective	Policy Statement
	information during and outside normal working hours. ➢ The relevant business owners shall communicate the Clear Desk and Clear Screen Policy to the employees in their own areas and periodically monitor their activities to ensure users compliance. ➢ Paper and computer media shall 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 documentation shall be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated. ➢ Sensitive or classified information, when printed, shall be cleared from printers immediately.

4. Network Access

Policy Objective	Policy Statement
Prevent unauthorized access to networked services [A.11.4]	➢ Prior to connecting any system to the network, checking against viruses and malwares shall be done and it shall be updated with the latest patches. ➢ If any kind of ambiguity is found in the user's workstation that requires access to the network; it shall be transferred to an isolated network. ➢ An antivirus solution shall be implemented to protect the network from malicious code. ➢ Network configuration shall be managed to restrict the access available for individual users to only those information assets for which they are authorized to access. ➢ User shall be giving access to the network resources according to Access Control and Access Management policies and related procedures. ➢ The use of network diagnostic and security tools shall be limited to specifically designated staff, and in accordance with their job responsibilities. ➢ Only network administrators shall be authorized to access network configuration and related security data. ➢ An updated network diagram shall be maintained. Periodic reviews shall be conducted by the Information Security Department 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. ➢ Users shall only be provided with the direct access to the services that they have been specifically authorized to use. ➢ Users shall not use dial-up modems for external connectivity, while they are connected to KAU internal network. ➢ All routing traffic shall be authorized based on business

Policy Objective	Policy Statement
	communications needs and in coordination with business process owners. ➢ Appropriate routing control mechanisms shall be deployed to restrict information flows to designated network paths within the control of KAU. ➢ Remote user access to KAU networks shall be subject to appropriate user authentication methods. ➢ All remote administration connection for maintenance, support and special services shall use strong authentication (as well as corresponding encryption methods to secure communication traversing the network. ➢ Internal, external and wireless networks shall be totally isolated by implementing separated security perimeter controls. ➢ Network connectivity from internal network to external network shall be adequately controlled, restricted and monitored by network administrators. ➢ Network-based Intrusion Prevention System (IPS) or Network-based Intrusion Detection System (IDS) shall be implemented in network segments domains based on KAU business requirements. ➢ All IPS/IDS policies and signature files shall be reviewed on a regular basis.

5. System Access

Policy Objective	Policy Statement
Prevent unauthorized access to operating systems [A.11.5]	➢ System shall be configured to run only restricted services as required. ➢ The logon process on any system shall display only the limited information about the system and its purposed use. ➢ System shall display a general notice warning that the computer should only be accessed by authorized users. ➢ During the logon procedure, system shall not provide help message that might aid an illegitimate users. ➢ 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. ➢ System shall limit the number of unsuccessful logon attempts allowed. ➢ During the logon procedure, system shall limit the maximum and minimum time allowed. If exceeded, the logon shall be terminated. ➢ Designated system administrators shall review the log of unsuccessful attempts in a periodically basis. ➢ Access to system utilities shall be strictly limited and controlled to prevent the potential of damage to KAU information.

6. Application Access

Policy Objective	Policy Statement
Prevent unauthorized access to information held in application systems [A.11.6]	➢ KAU shall restrict access to information and application system functions. ➢ Security controls shall be defined to control outputs from application systems that handle sensitive information. ➢ Physical and/or logical isolation for sensitive systems shall be defined. ➢ Sensitive application that handles sensitive data shall be run on a dedicated operating system. ➢ Application shall be configured to run only limited services as per KAU requirements.

7. Mobile Access

Policy Objective	Policy Statement
Ensure information security when using mobile computing and teleworking facilities [A.11.7]	➢ KAU shall define and implement appropriate security controls to protect against the risks of using mobile computing and communication facilities. ➢ KAU shall adopt formal and documented procedures against malicious software. ➢ Remote access to business information across public network using mobile computing facilities shall only take place after successful identification and authentication, and with suitable access control mechanisms in place. ➢ When travelling, equipment and media shall not be left unattended in public places. ➢ Appropriate security arrangements and controls shall be in place before teleworking activities are authorized. ➢ When the teleworking activities are completed, revocation of authority and access rights, and the return of equipment shall be done immediately. ➢ An accurate and up to date record of all the teleworking activities shall be maintained. ➢ All mobile users shall take an adequate care when mobile computing facilities are used in public areas, meeting rooms and other unprotected areas. ➢ Loss of any mobile device containing sensitive data or any other security breach shall be immediately reported to Information Security Department. ➢ Laptops and home personal computers shall not be used for business activities without appropriate authorization from IT Dean and applying the appropriate security control, including up to date security “patches” and virus protection.

Policy Objective	Policy Statement
	➢ Users shall understand their responsibility toward equipment, all data and information held or stored on the equipment.

Glossary

Asset	Anything that has value to the organization
Availability	The property of being accessible and usable upon demand by an authorized entity
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, IT Dean, or legal nature Note: Control is also used as a synonym for safeguard or countermeasure
Employee Hand Book	A documentation including instructions and information that employees shall abide or shall need to refer to in order to meet the terms and conditions of their employment
Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies
Information Processing Facilities	Any information processing system, service or infrastructure, or the physical locations housing them
Information Security	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
Information Security Event	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
IRC	Incident Reporting Contact is responsible for receiving and logging all reported IT incidents
IRT	Incident Response Team is a group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations
IRTL	Incident Response Team Leader
ISMS	An Information Security Management System is a set of policies concerned with information security management.
KAU	King Abdulaziz University
Mobile Code	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
Service-Level Agreement (SLA)	It is a negotiated agreement between two parties where one is the customer and the other is the service provider
Policy	Overall intention and direction as formally expressed by management
Risk	Combination of the probability of an event and its consequence
Risk Analysis	A systematic use of information to identify sources and to estimate risk
Risk Assessment	Overall process of risk analysis and risk evaluation
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
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
Risk Treatment	Process of selection and implementation of measures to modify risk
Third Party	That person or body that is recognized as being independent of the parties involved, as concerns the issue

	in question
Threat	A potential cause of an unwanted incident, which may result in harm to system or organization
Vulnerability	A weakness of an asset or group of assets that can be exploited by a threat