Policy of Information Handling
in
Qassim University

Prepared by:
Deanship of Development and Quality
2019

Policies Related to the Electronic Gate

Portal Concepts

- The portal is the Website of Qassim University and all its content publishing sites, whether it is a college site, a deanship, a department, or a website for a faculty member, employee or student.
- Terms of Use are all terms and conditions that must be taken into account when using the portal at the University of Qassim.
- Content is text, graphs, advertisements, links or other materials such as University news, University events, visuals, University staff contact data, courses and published articles.
- External links are links that navigate to non-Qassim University Portal pages.

Terms of use

- The portal is the only official site of Qassim University and is managed by the Deanship of Information Technology represented by the Department of Software and the management of the electronic portal, and the content is managed through deanships, colleges, departments and University centers and both expressing itself.
- Qassim University should make available the terms of use of the portal on all portal pages.
- The user must know that his use of Qassim University Portal is an acceptance of the terms of use of the portal, if the user does not accept it fully, access to this site or any sub-site is infringing and must stop using it immediately.

Reservation of subdomains

- Qassim University web sites must be hosted through the University, through other government entities, or through hosting providers licensed by the CITC. Hosting shall be within the Kingdom, and the contract between the parties shall include controls to ensure the confidentiality of the information.
- Each entity in the University has the right to reserve a domain or a short name to be affiliated with the University domain ((qu.edu.sa) by submitting an official letter to the (Deanship of Information Technology) stating the short name to be reserved.
- No entity at the Qassim University can create a website outside the domain (qu.edu.sa).

Content entry and update validity

- The responsibility of adding, deleting or modifying the tabs in the main portal of the University Portal is the responsibility of the Department of Software and the electronic portal of the Deanship of Information Technology at Qassim University or its designee.
- The responsibility of the management of the electronic newspaper of the University lies with the Media and Communication Center at the University, where it has full authority to publish and update the contents of the electronic newspaper as well as everything related to news, events, seminars, conferences, articles and the services under it.
- Any party in Qassim University who wishes to publish news, events, seminars, articles or conferences on the main page of the University portal has to communicate with the University's Media and Communication Center formally.
- In the case of the need to add something to the software (such as adding an attendance registration form), the Software and e-Portal Section of the Deanship of Information Technology must be provided with an official letter via administrative means containing applications not less than three weeks prior to the date of the conference or event. Otherwise, the application will not be considered.
- Each entity of the University has an independent site with the authority to manage it completely, so the responsibility of publishing and updating the electronic content of each entity on the dean or director of the responsible entity and is responsible for publishing and updating the entire contents, and each faculty member or employee or student have an independent site.
- The Deanship of Information Technology is not committed to reviewing external links related to the portal. The Deanship is not responsible for the content or services provided by sites registered outside the scope of the official portal of the University.

Posting on the portal

- The portal is an electronic means of publishing for all University employees and sectors and they should use them for the benefit of the University and its employees and its various sectors and in no way prejudice the reputation of the University and its employees or expose them to legal accountability.
- All content published on the portal pages must comply with the copyright, and therefore the following should not be published without limitation:

- Any electronic material not owned by the owner of the page and has copyright.
- Research published in scientific conferences and scientific journals.
- Books and literature available in any electronic format.
- Inappropriate content, including but not limited to:
- Any material that contains an offensive, aggressive, racist or threatening tone, whether text, picture or idea.
- Any material that violates the regulations of the state and University or customs of society.
- Any material that violates the privacy of others in any way.

• Each party of the University that has a site belonging to the University gate has to make sure to update the content of pages and materials, including news, contact information, phone numbers, e-mail and description of materials and other information.

• Everyone should use the proper grammar of the language used in creating the page or electronic material and make sure it is correct and error-free.

• Deanship of Information Technology reserves the right to change or delete the information contained in any site under the umbrella of the University at any time without giving a notice in the event of any violation of the portal policies for publishing and content management.

Privacy

• The Deanship of Information Technology at Qassim University should make the privacy policy available on all pages of the portal, to clarify the rights and duties of the University site and its affiliates and users, and therefore University of Qassim is committed to protecting the confidentiality and privacy of the user.

• Privacy policies contain how Qassim University treats personal user information regarding data, whether online or on computers only.

• Some of the links on Qassim University site link to other non-university sites (not in the domain of qu.edu.sa). These sites do not operate in accordance with the privacy policy of the Qassim University site. Therefore, whoever visits those sites should review the privacy policy of those sites before disclosing any personal information indicating their owner.

Supervision and Training

- Each party has the right to allocate one or more supervisors that belongs to them, where this supervisor is granted the necessary roles on his university account used in the access system and is thus responsible for the website of the entity and its content and all the necessary tasks to ensure the continuity of work on the site.
- The Deanship of Information Technology is committed to providing the necessary training for the management of the website (for any entity that has a website under the umbrella of the portal).
- Every faculty member and the like at the University are entitled to the training required to manage their personal pages under the faculty pages.
- Faculty members and the like have the right to receive the necessary training to manage their personal pages within the pages of faculty members or the sites of the bodies, in coordination with the Deanship of Information Technology directly.

Internal network (SSL VPN) Policies at Qassim University

- VPN connection is allowed only when necessary and for the following persons:
  - o Anyone who has the authority to provide emergency technical support on one of the University's electronic systems.
  - o The System administrator determined by the business owner.
  - o The approved suppliers from the Deanship of Information Technology after the necessary supplies and installations.
- The service is requested according to the pre-defined workflow plan approved by the Dean of IT.
- The Deanship of Information Technology must encrypt the personal account used to connect to the University network through the SSL VPN service while crossing over unsecured and reliable networks.
- The complexity and difficulty requirements for passwords must be met in accordance with the user password management policy.
- Employees authorized by the University must ensure that unauthorized users are not allowed to share the University's VPN services, obtain their password, or access and use the computer during the connection process.

- All computers connected to the University network are secured through the VPN service in accordance with the standards of the Deanship of Information Technology for anti-virus programs with the latest versions of their files as well as the latest update of security patches for the operating system.
- Only approved computer communication applications can be used to open channels of communication to the University network through the VPN service.
- Authorized staff members will be automatically disconnected from the University network via VPN after one hour of inactivity.
- Computers are subject to employees authorized to access the network through the VPN service according to their business needs to restrict access to the network.
- The Deanship of Information Technology should examine, monitor and review all VPN channels in Qassim University.
- It is forbidden to grant a VPN connection if the beneficiary is outside the Kingdom of Saudi Arabia except in cases of necessity.
- The Deanship of Information Technology has the right to monitor, limit or disconnect any VPN connection for any purpose without prior notice.

VPN service can be requested at:

https://eservices.qu.edu.sa

Password Policy

- Whenever there is a temporary or a permanent termination of Qassim University's relationship with an employee, client or partner who has access to Qassim University assets, user access and privileges shall be immediately revoked.
- Whenever there is a temporary or a permanent termination of Qassim University's relationship with an employee, client or partner who has access to Qassim University assets, user access and privileges shall be immediately revoked.
- Default passwords shall be changed when new assets are acquired, before connecting it to Qassim University infrastructure and placing it in production environment.
- During the login procedure on Qassim University information systems, the password shall not be displayed on screen. When typing the password, the user shall make sure that he is not watched and the entry field of password shall display a common symbol (e.g. a star) for every typed character (password masking).
- Username locking and password expiry shall be defined based on the assets classification and security requirements.
- Simple and privileged users, whenever possible, shall use separate passwords for every assets they have access to. In case of a user central management infrastructure (e.g. Single Sign On) the implementation of a two-factor authentication approach shall be considered.
- User and administrator shall follow the following security characteristics when choosing passwords:
    - They shall be at least eight (8) characters long.
    - Password shall be combination of alphanumeric characters (both upper and lower case characters) and numbers and symbols.
    - Password shall not contain all of the username.
    - Remember password option shall not be activated.
- User account shall be locked for 15 minutes after five unsuccessful attempts.
- For every system manager of IT systems, password change shall be enforced by domain control at least every (120) days.

- For every user of IT systems users', password change shall be enforced by domain control at least every (180) days at least every (120) days.
- Passwords shall not be stored on systems or transferred over networks (internal or external) without being encrypted.
- All assets access related passwords shall be changed immediately if there is suspicion or proof that passwords have been revealed to unauthorized users.

Password Use:

- Information users shall follow Qassim University security practices in the selection and use of passwords according to User Password Management.
- Information users shall not share their username and password with others; thus they will be accountable for any activity associated with their access.
- All Information users shall check the activities of their accounts as reported by the system, i.e. last login times, and report in a timely manner if any abnormal activity found.

Password Management System:

- Qassim University shall adopt an interactive system for managing passwords in order to ensure the quality of passwords and compliance with User Password Management Policy.

Backup Policy

- Deanship Management of IT through close interaction and coordination with the asset's owners shall identify a Backup and Restoration Plan of all Qassim University assets in line with:
    - Legal and regulatory requirements.
    - Assets classification.
    - Vendor recommendations
- The Backup and Restoration Plan shall determine the following:
    - Backup type.
    - Backup schedule.
    - Backup Protection (based on the classification of the information backed up).
    - Backup Retention.
- Backed up data shall be checked and tested regularly. (quarterly) to ensure that its integrity and effectiveness through restoration of selective data.
- Restoration of backups will require specific and appropriate authorization from asset owner and shall be performed in accordance with the Backup and Restoration Procedure.
- The backup media shall be replaced immediately after encountering an error or at predefined time intervals whichever is earlier.
- Backup media shall be appropriately labelled and numbered automatically by the backup system, whenever possible, or manually by the system administrator Backup media shall have at least the following identifying criteria that can be readily identified by labels system:
    - System name.
    - Creation Date
    - Classification.
    - Retention period of taking the backup.

- Storage of backup:
    - On-site: On-site data backup must be maintained in safe custody, preferably outside the server room and in a safe cabinet. (The storage is currently inside the server room without an independent cabins)
    - Off-site: Whenever possible, Off-site data backup must be maintained at off-site location. (it is not available now)
- Backup logs shall be reviewed by the respective System Administrator to ensure proper backup.
- The backup logs shall be maintained and kept up-to-date.
- Wherever possible, backup that contain information classified as CONFIDENTIAL" and above shall be encrypted.

Systems Use Policy

- All systems in Qassim University must follow the policy of acceptable use of assets.
- Any change to systems shall follow change management procedure.
- All systems in Qassim University must follow the information backup policy.
- System owner shall be responsible for defining the following, but not limited to:
    - User access groups.
    - User access rights.
- User access request shall be duly approved by the System owner and requester department manager before assigning privileges to the information users.
- Access to System shall be provided to information users to perform their business related activities. Furthermore, access shall be provided on a need-to-know /least privilege basis.
- Access rights (privileges) shall be recorded in an access control list. Such records shall be regarded as confidential documents and safeguarded accordingly.

- Information users IDs that indicate the privileges level of the users, (e.g. user ID of 'root or admin'), shall be avoided.
- Access to Qassim University System shall be controlled by appropriate security mechanisms in relation to the following:
    - Level of Trust (trusted, semi-trusted and un-trusted).
    - Access Level (simple or privileged access).
    - Access Type (internal, remote or access to third party systems)
- User access and privileges shall be reviewed at least once a year by the System owner in cooperation with IT Deanship.
- Reviewing users' access and privileges shall be in relation with the changes to the system involved, changes to location and regulatory compliance requirements.
- Qassim University shall monitor the following events and make provision for expert analysis of this data to discover anomalies, potential vulnerabilities or security incidents:
- System owner shall monitor the following:
    - Logon and logoff success and failure
    - Restart, shutdown, system success and failure
    - Security policy changes success and failure
    - User and group management success and failure
    - File and object access success and failure
    - Use of user rights success and failure
- Deanship Management of IT shall monitor the following:
    - Departures from 'normal' usage patterns, such as:
    - System load at different times of the day
    - Number of processes running
    - CPU utilization
    - Unusual successes/denials of connections
    - Success and error messages from firewalls

- Multiple access attempts

Access to unusual ports ○

- Qassim University shall ensure that information security controls in place, are affective, and not being bypassed. Monitoring shall consist of activities such as, but not limited, the review of:
  - Intrusion detection system logs
  - Firewall logs o User account logs
  - Network scanning logs
  - Application security logs
  - Security log
- Qassim University shall review the results of monitoring activities according to the risks involved. The following risk factors, but not limited to, shall be considered:
  - Criticality of the assets involved.
  - Past experience of system penetration and misuse, and the frequency of vulnerabilities being exploited.
  - Extent of system interconnection (particularly public networks).
  - Logging facility being de-activated
- Qassim University shall ensure the validity and integrity of data input to application by:
  - Limiting fields to accept specific ranges of data (e.g., defining out of range values or upper and lower data volume limits).
  - Checking for invalid characters in data fields.
  - Making key fields mandatory.
  - Verifying the acceptability of input data using business rules.
  - Protecting against common attacks (e.g., buffer overflows, DOS, DDoS).
  - Using control balances to verify complete input and processing.
- The results of the data processing shall be checked to verify their accuracy. The following shall be applied as a minimum:

- Check on results to identify invalid values (e.g. control characters) and to prevent attacks such as Cross Site Scripting.
- Check on the results classification to verify correct classification assignment (e.g. confidential data shall not be accessible by Un-Trusted Users).
- Error handling procedures shall be in place to avoid presenting detailed error messages to users

QU Saudi Arabia

Qassim University جامعة القصيم

رؤية VISION 2030

المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

Policy of Information Handling