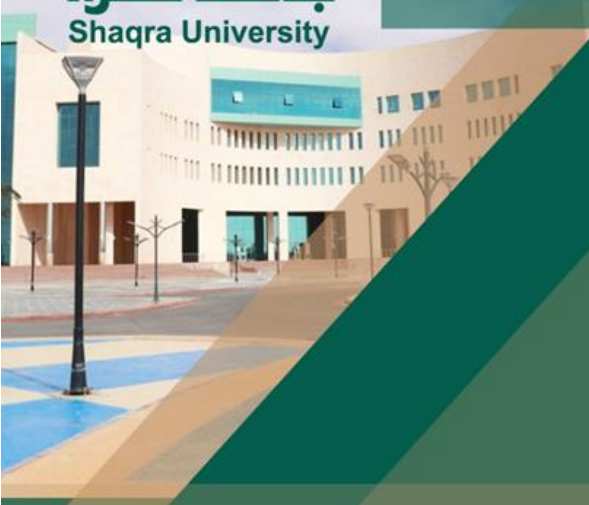
جامعة شقراء
Shaqra University

إدارة الأمن السيبراني
Cyber Security Department



Asset Acceptable Use Policy

Shaqra-CS-P-005	Document Code
V 1.1	Version
07/05/2024	Version Date
Green	TLP

Traffic Light Protocol (TLP)

The Traffic Light Protocol (TLP) system was created to facilitate the sharing of sensitive information and is widely used around the world. There are four colors (traffic signals) in this system:

Red – Personal and Confidential for the Recipient Only

The recipient is not permitted to share information classified with a red signal with any individual, whether inside or outside the organization, beyond the specified scope of receipt.

Amber – Limited Sharing

is for information that should be shared within the organization and with trusted partners.

Green – Sharing within the Same Community

The recipient is allowed to share information classified with a green signal within their organization or with another organization that has a relationship or within the same sector. It is not permitted to exchange or disseminate it through public channels.

White – Unlimited

Table of Contents

Purpose

This policy aims to define the requirements related to acceptable use in Shaqra University in order to minimize the cybersecurity risks resulting from internal and external threats to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy applies to all information and technology assets in the Shaqra University and applies to all personnel (employees and contractors) in the Shaqra University.

Policy Statements

1- **General Requirements**

1-1 Cybersecurity requirements must be followed in the policies, standards, and procedures approved by Shaqra University.

1-2 Data and assets (hardware, information, or software) must be protected and handled as per their sensitivity and classification in accordance with the Data Protection Policy approved by Shaqra University. Also, data confidentiality, integrity and availability must be ensured.

1-3 No printed matters should be left unattended on the shared printer.

1-4 External storage media must be kept in a secure and appropriate manner, such as ensuring that the temperature is set at a certain degree and stored in an insulated and safe place.

1-5 It is prohibited to disclose any of the Shaqra University information, including systems and networks related information, to any unauthorized entity or party, whether internal or external.

1-6 It is prohibited to publish information about the Shaqra University via the media and social media networks without permission of the Authorizing Official.

1-7 It is prohibited to use the Shaqra University systems and assets to achieve personal benefit and business, or for any purpose not related to the activity and works of Shaqra University.

1-8 It is prohibited to connect personal devices to networks and systems of Shaqra University without prior authorization from the Cybersecurity Department. This should be done in accordance with Workstations, Mobile Devices and BYOD Security Policy approved by Shaqra University.

1-9 It is prohibited to perform any activities intended to bypass the Shaqra University protection systems, including anti-virus programs, firewall, and malware without prior authorization, and in accordance with the procedures approved by Shaqra University.

1-10 The Cybersecurity Department retains its right to monitor and periodically review work-related systems, networks and personal devices, in order to monitor compliance with cybersecurity policies and standards approved by Shaqra University.

1-11 The Cybersecurity Department must be notified in case of loss, theft or leakage of Shaqra University information.

1-12 Information and Asset Acceptable Use rules related to Information Processing systems must be followed up.

1-13 All Shaqra University employees and staff must return all files, documents, information and assets in their possession upon work completion or expiry of their contract/agreement.

1-14 It is prohibited to transfer assets off-site without prior permission from relevant departments.

1-15 Assets that are off-site must be protected taking into account the various risks of working outside Shaqra University buildings.

1-16 Sessions, meetings and contents related to security awareness campaigns organized by the Shaqra University must be attended and should be abided by.

1-17 All staff must sign a statement of consent on Asset Acceptable Use approved by Shaqra University.

1-18 All staff must approve and acknowledge the Code of Conduct and Acceptable Use Policy upon any review or update thereof.

1-19 Access to Shaqra University assets must be according to roles and responsibilities required to perform tasks only.

1-20 Technical asset administrators must be alerted about cybersecurity patches to be implemented according to Shaqra University Patch Management Policy.

1-21 Asset owners must review user access rights at defined and regular intervals.

1-22 The Cybersecurity Department must be notified when suspecting any activity that may harm Shaqra University or its assets, such as suspected sites, cybersecurity risks or mail contents that may harm Shaqra University.

1-23 In case of non-compliance with any item, Shaqra University must explain and state the reasons.

1-24 Key performance indicators (KPIs) must be used to ensure correct and effective use of requirements and protect Shaqra University information and technology assets.

2- Protection of Laptops

2-1 It is prohibited to use external storage media without prior authorization from Cybersecurity Department. When used, stored data must be encrypted according to Shaqra University Encryption Standard.

2-2 Devices must be secured before leaving office by Sign out or Lock, whether leaving for a short time or after working hours.

2-3 It is prohibited to use or install hardware, tools, or applications unapproved by Shaqra University on the laptop without prior authorization of Deanship of E-learning and Digital Transformation.

3- Internet and Software Acceptable Use

3-1 Security messages that may arise while browsing the internet or internal networks must be treated cautiously and be dealt with only after contacting Cybersecurity Department.

3-2 It is prohibited to violate the rights of any person, or company protected by copyright, patent or other intellectual property, similar laws or regulations, including, but not limited to, installation of unauthorized or illegal software for any business purposes, or use of external storage media without consent of Shaqra University.

3-3 A secure and authorized browser must be used to access internal network or internet.

3-4 It is prohibited to use techniques that allow bypassing Proxy or Firewall to access Internet.

3-5 It is prohibited to upload or install Software and tools on Shaqra University assets without prior authorization of Cybersecurity Department.

3-6 It is prohibited to use Internet for non-business purposes, including uploading media and files, as well as using file sharing software without prior authorization of Cybersecurity Department.

3-7 It is prohibited to conduct a security check to discover security vulnerabilities, including penetration testing, or monitoring Shaqra University networks and systems, or third-party networks and systems without prior authorization of Cybersecurity Department.

4- Email Acceptable Use

4-1 It is prohibited to use email, telephone or e-fax for non-business purposes, noting that their use shall only be in accordance with cybersecurity policies and standards approved by Shaqra University.

4-2 It is prohibited to exchange messages containing inappropriate or unacceptable content, including messages with internal and external parties.

4-3 Encryption techniques must be used when sending sensitive information via email or communication systems as per the Shaqra University Data Protection Policy.

4-4 Shaqra University email address should not be registered at any site not related to work.

4-5 Shaqra University has the right to disclose emails' content after obtaining the necessary permits from the Representative and the Cybersecurity Department in accordance with the Shaqra University's relevant approved procedures and regulations.

4-6 It is prohibited to open suspicious or unexpected emails and attachments, even if they appear to be from reliable sources.

5- Video Conferences and Web-based Communications

5-1 It is prohibited to use unauthorized tools or software to make calls or hold video conferences related to work.

5-2 It is prohibited to make calls or hold video conferences not related to work without prior authorization to use Shaqra University's tools or software.

5-3 It is prohibited to hold meetings related to work in public places due to risk of leaking classified information.

6- Passwords Use

6-1 It is necessary to choose secure passwords and to safeguard Shaqra University systems and assets passwords in accordance with Shaqra University Identity and Access Management Policy. It is also necessary to choose passwords different from those of personal accounts, such as personal mail and social media accounts.

6-2 It is prohibited to share the password by any means, including electronic correspondence, voice calls, and paper writing. Users must not disclose passwords to any other party, including co-workers and employees of Deanship of E-learning and Digital Transformation and immediately notify Cybersecurity Department immediately if this occurs.

6-3 Passwords must be changed on a regular basis according to Password Policy requirements or upon obtaining a new password from the system administrator.

6-4 It is prohibited to use previously used or common passwords. It is also prohibited to share user's password with anyone.

7- **Office Use**

7-1 It is necessary to abide by Shaqra University's Secure and Clean Office Policy, and to make sure the desktop and screen are free of classified and sensitive information as per Shaqra University's approved classifications.

7-2 It is prohibited to leave any Shaqra University classified or sensitive information in places that are easily accessible, or accessed by unauthorized persons.

7-3 It is prohibited to leave office doors and cabinets containing classified and sensitive information open.

8- **Cloud Computing**

8-1 Data must be classified prior to being hosted with cloud computing and hosting service providers, and returned to the organization (in a usable format) upon service completion.

8-2 Shaqra University environment (especially virtual servers) must be separated from other cloud computing environment of other organizations.

8-3 Location for hosting and storing Shaqra University information must be inside the Kingdom and storing must be in accordance with the relevant legal and regulatory requirements.

8-4 Cybersecurity requirements for protection of cloud computing subscribers' data and information must be covered in accordance with the relevant legal and regulatory requirements, as a minimum:

8-5-1 Guarantees for ability to delete data safely upon expiry of relationship with service provider (Exit Strategy).

8-5-2 Use secure means to export and transfer data and virtual infrastructure.

Roles and Responsibilities

1- **Policy Owner:** Cybersecurity Management Director

2- **Policy Review and Update:** Cybersecurity Department

3- **Policy Implementation and Execution:** Human Resources

4- **Policy Compliance Measurement**: Cybersecurity Department

Update and Review

Cybersecurity Department must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in Shaqra University or the relevant regulatory requirements.

Compliance

1- The Cybersecurity Management Director will ensure compliance of Shaqra University with this policy on a regular basis.

2- All personnel at Shaqra University must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action as per Shaqra University's procedures.