Understanding AUP

Acceptable Use Policy: An AUP outlines the guidelines and expectations for using an organization's technology resource. It help protect the organization from security issues, misuse of information, and even avoid legal issues. Employees and users are expected to understand what behaviors are appropriate according to the company's guidelines.

Acceptable vs Unacceptable Behaviors

Category	Acceptable Behavior	Unacceptable Behavior
Internet Usage	Accessing Work related websites.	Visiting inappropriate, offensive, or illegal websites
Email Communication	Work related emails with colleagues and company employees	Sending spam and phishing emails.
Software	Installing and usage of only company approved software's	Downloading illegal or APk software's which are unauthorized.
Device Usage	Using strong passwords and biometrics to keep company devices secure.	Using personal devices on company's network.
Social Media	Positively representing and promoting the company online.	Engaging in harassing and detegoratory speeches.

Acceptable Use Policy

Purpose

The purpose of **Quantum Lab Acceptable Use Policy (AUP)** is to establish clear guidelines for the appropriate use of company-owned devices, networks, and internet resources. This policy aims to protect company assets, ensure compliance with legal and regulatory requirements, and promote a secure and productive work environment.

Audience

The Quantum Lab Acceptable Use Policy applies to any individual, entity, or process that interacts with any Quantum Lab **Information Resource**.

Contents

This policy applies to all employees, contractors, and third-party users who access the company's information systems, including but not limited to:

- Company-owned computers, mobile devices, and other hardware

- Internet and intranet access

- Email and communication platforms

- Social media accounts used for business purposes

Policy

Acceptable Use

- Personnel are responsible for complying with Quantum Lab policies when using Quantum Lab information resources and/or on Quantum Lab time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Department.
- Personnel must promptly report harmful events or policy violations involving Quantum Lab assets or information to their manager or a member of the Incident Handling Team. Events include, but are not limited to, the following:
  - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in business availability to Quantum Lab **Information Resources**.
  - Data incident: any potential loss, theft, or compromise of Quantum Lab information.
  - Unauthorized access incident: any potential unauthorized access to a Quantum Lab **Information Resource**.
  - Facility security incident: any damage or potentially unauthorized access to a Quantum Lab owned, leased, or managed facility.
  - Policy violation: any potential violation to this or other Quantum Lab policies, standards, or procedures.
- Personnel should not purposely engage in activity that may
  - harass, threaten, impersonate, or abuse others;
  - deteriorate the performance of Quantum Lab **Information Resources**;
  - deprive authorized Quantum Lab personnel access to a Quantum Lab **Information Resource;**
  - obtain additional resources beyond those allocated;
  - or circumvent Quantum Lab computer security measures.
- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, Quantum Lab personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Quantum Lab **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on Quantum Lab time and/or using Quantum Lab **Information Resources** are the property of Quantum Lab.
- Use of encryption should be managed in a manner that allows designated Quantum Lab personnel to promptly access all data.
- Quantum Lab **Information Resources** are provided to facilitate company business and should not be used for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using Quantum Lab **Information Resources**.
- Personnel should not intentionally access, create, store or transmit material which Quantum Lab may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a "**need to know**".
- Personnel are permitted to use only those network and host addresses issued to them by Quantum Lab IT and should not attempt to access any data or programs contained on Quantum Lab systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal Quantum Lab networks and/or environments must be made through approved, and Quantum Lab-provided, virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information, including IT support personnel.
- Personnel must not share their (personal authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Multi-factor authentication information
    - Access cards and/or keys,
    - Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Access cards and/or keys that are no longer required must be returned to physical security personnel.
- Lost or stolen access cards, security tokens, and/or keys must be reported to physical security personnel as soon as possible.
- A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following Quantum Lab rules:
    - Must meet all requirements including minimum length, complexity, and reuse history.
    - Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
    - Must not be the same passwords used for non-business purposes.
- Unique passwords should be used for each system, whenever possible.
- User account passwords must not be divulged to anyone. Quantum Lab support personnel and/or contractors should never ask for user account passwords.
- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Quantum Lab, if issued.

Clear Desk/Clear Screen

- Personnel should log off from applications or network services when they are no longer needed.

- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Confidential or internal information should be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- Personal items, such as phones, wallets, and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.
- File cabinets containing **confidential information** should be locked when not in use or when unattended.
- Physical and/or electronic keys used to access **confidential information** should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Laptops should be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Copies of documents containing **confidential information** should be immediately removed from printers and fax machines.

Data Security

- Personnel should use approved encrypted communication methods whenever sending **confidential information** over public computer networks (Internet).
- **Confidential information** transmitted via USPS or other mail service must be secured in compliance with the Information Classification and Management Policy.
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- **Confidential information** must be transported either by an Quantum Lab employee or a courier approved by IT Management.
- All electronic media containing confidential information must be securely disposed. Please contact IT for guidance or assistance.

Email and Electronic Communication

- Auto-forwarding electronic messages outside the Quantum Lab internal systems is prohibited.
- Electronic communications should not misrepresent the originator or Quantum Lab.
- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Accounts must not be shared without prior authorization from Quantum Lab IT, with the exception of calendars and related calendaring functions.
- Employees should not use personal email accounts to send or receive Quantum Lab **confidential information**.
- Any personal use of Quantum Lab provided email should not:
  - Involve solicitation.
  - Be associated with any political entity, excluding the Quantum Lab sponsored PAC.

- o   Have the potential to harm the reputation of Quantum Lab.
- o   Forward chain emails.
- o   Contain or promote anti-social or unethical behavior.
- o   Violate local, state, federal, or international laws or regulations.
- o   Result in unauthorized disclosure of Quantum Lab **confidential information**.
- o   Or otherwise violate any other Quantum Lab policies.
- Personnel should only send **confidential information** using approved secure electronic messaging solutions.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing **confidential** or **internal information** in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

Hardware and Software

- All hardware must be formally approved by IT Management before being connected to Quantum Lab networks.
- Software installed on Quantum Lab equipment must be approved by IT Management and installed by Quantum Lab IT personnel.
- All Quantum Lab assets taken off-site should be physically secured at all times.
- Personnel traveling to a High-Risk location, as defined by FBI and Office of Foreign Asset control, must contact IT for approval to travel with corporate assets.
- Employees should not allow family members or other non-employees to access Quantum Lab **Information Resources**.

Internet

- The Internet must not be used to communicate Quantum Lab **confidential** or **internal information**, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with Quantum Lab networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
  - o   Recreational games,
  - o   Streaming media,
  - o   Personal social media,
  - o   Accessing or distributing pornographic or sexually oriented materials,
  - o   Attempting or making unauthorized entry to any network or computer accessible from the Internet.
  - o   Or otherwise violate any other Quantum Lab policies.
- Access to the Internet from outside the Quantum Lab network using a Quantum Lab owned computer must adhere to all of the same policies that apply to use from within Quantum Lab facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- Quantum Lab does not allow **personally owned mobile devices** to connect to the Quantum Lab corporate internal network.

OR

- The use of a **personally owned mobile device** to connect to the Quantum Lab network is a privilege granted to employees only upon formal approval of IT Management.
- All **personally owned** laptops and/or workstations must have approved virus and spyware detection/protection software along with personal firewall protection active.
- Mobile devices that access Quantum Lab email must have a PIN or other authentication mechanism enabled.
- **Confidential information** should only be stored on devices that are encrypted in compliance with the Quantum Lab Encryption Standard.
- Quantum Lab **confidential information** should not be stored on any personally owned **mobile device**.
- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to the Quantum Lab Security Team immediately.
- All **mobile devices** must maintain up-to-date versions of all software and applications.
- All personnel are expected to use **mobile devices** in an ethical manner.
- **Jail-broken** or rooted devices should not be used to connect to Quantum Lab **Information Resources**.
- Quantum Lab IT Management may choose to execute "**remote wipe**" capabilities for **mobile devices** without warning (see Mobile Device Email Acknowledgement).
- In the event that there is a suspected **incident** or breach associated with a **mobile device**, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to Quantum Lab **Information Resources** may be monitored, at the discretion of Quantum Lab IT Management.
- Quantum Lab IT support for **personally owned mobile devices** is limited to assistance in complying with this policy. Quantum Lab IT support may not assist in troubleshooting device usability issues.
- Use of **personally owned** devices must be in compliance with all other Quantum Lab policies.
- Quantum Lab reserves the right to revoke **personally owned mobile device** use privileges in the event that personnel do not abide by the requirements set forth in this policy.
- Texting or emailing while driving is not permitted while on company time or using Quantum Lab resources. Only hands-free talking while driving is permitted, while on company time or when using Quantum Lab resources.

Physical Security

- Photographic, video, audio, or other recording equipment, such as cameras and cameras in **mobile devices**, is not allowed in secure areas.
- Personnel must display photo ID access card at all times while in the building.
- Personnel must badge in and out of access-controlled areas. Piggy-backing, tailgating, door propping and any other activity to circumvent door access controls are prohibited.
- Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times.
- Eating or drinking are not allowed in data centers. Caution must be used when eating or drinking near workstations or information processing facilities.

Privacy

- Information created, sent, received, or stored on Quantum Lab **Information Resources** are not private and may be accessed by Quantum Lab IT employees at any time, under the direction of Quantum Lab executive management and/or Human Resources, without knowledge of the user or resource owner.
- Quantum Lab may log, review, and otherwise utilize any information stored on or passing through its **Information Resource** systems.
- Systems Administrators, Quantum Lab IT, and other authorized Quantum Lab personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment related task.

Removable Media

- The use of **removable media** for storage of Quantum Lab information must be supported by a reasonable business case.
- All **removable media** use must be approved by Quantum Lab IT prior to use.
- **Personally, owned removable media** use is not permitted for storage of Quantum Lab information.
- Personnel are not permitted to connect **removable media** from an unknown origin without prior approval from the Quantum Lab IT.
- Confidential and internal Quantum Lab information should not be stored on **removable media** without the use of encryption.
- All removable media must be stored in a safe and secure environment.
- The loss or theft of a **removable media** device that may have contained any Quantum Lab information must be reported to the Quantum Lab IT.

Security Training and Awareness

- All new personnel must complete an approved **security awareness** training class prior to, or at least within 30 days of, being granted access to any Quantum Lab **Information Resources**.
- All personnel must be provided with and acknowledge they have received and agree to adhere to the Quantum Lab Information Security Policies before they are granted to access to Quantum Lab **Information Resources**.
- All personnel must complete the annual security awareness training.

Social Media

- Communications made with respect to social media should be made in compliance with all applicable Quantum Lab policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent Quantum Lab, including accounts that could reasonably be assumed to be an official Quantum Lab account, requires the permission of the Quantum Lab Communications Departments.
- When discussing Quantum Lab or Quantum Lab -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an Quantum Lab representative, and
    - Make it clear that you are speaking for yourself and not on behalf of Quantum Lab, unless you have been explicitly approved to do so.

- Personnel should not misrepresent their role at Quantum Lab.
- When publishing Quantum Lab-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; "The opinions and content are my own and do not necessarily represent Quantum Lab's position or opinion."
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with Quantum Lab will not be tolerated.
- **Confidential information**, internal communications and non-public financial or operational information may not be published online in any form.
- Personal information belonging to customers may not be published online.
- Personnel approved to post, review, or approve content on Quantum Lab social media sites must follow the Quantum Lab Social Media Management Procedures.

VoiceMail

- Personnel should use discretion in disclosing **confidential** or **internal information** in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.
- Personnel should not access another user's voicemail account unless it has been explicitly authorized.
- Personnel must not disclose **confidential** information in voicemail messages.

Incidental Use

- As a convenience to Quantum Lab personnel, incidental use of **Information Resources** is permitted. The following restrictions apply:
  - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to Quantum Lab approved personnel; it does not extend to family members or other acquaintances.
  - Incidental use should not result in direct costs to Quantum Lab.
  - Incidental use should not interfere with the normal performance of an employee's work duties.
  - No files or documents may be sent or received that may cause legal action against, or embarrassment to, Quantum Lab or its customers.
- Storage of personal email messages, voice messages, files and documents within Quantum Lab **Information Resources** must be nominal
- All information located on Quantum Lab **Information Resources** are owned by Quantum Lab may be subject to open records requests and may be accessed in accordance with this policy.

References
- ISO 27002: 6, 7, 8, 9, 11, 12, 13, 16, 18
- NIST CSF: PR.AC, PR.AT, PR.DS, DE.CM, DE.DP, RS.CO
- Asset Management Policy
- Encryption Management Policy
- Encryption Standard

- Identity and Access Management Policy
- Incident Management Policy
- Information Classification and Management Policy
- Mobile Device Acknowledgement
- Personnel Security and Awareness Policy
- Physical Security Policy
- Social Media Management Procedure

NEED HELP?

Quantum Lab is a full-service information security consultancy.

If you need assistance with anything in this resource, please don't hesitate to reach out to us.

CONTACT US

(314) 679 – 0786 | 4124 Lindell Blvd, Saint Louis, 63108