



# ISMS Acceptable Usage Policy

Version 1.0

## Version Control

Date	Version	Author	Changes
01-06-2025	1.0	Aditya	Document created

## Approved by CEO

01-06-2025

---

Signature

---

Date

1. Purpose-----	4
2. Scope -----	4
3. Audience -----	4
4 Definition-----	4
5. Acceptable use of Information assets-----	5
5.1 Purpose-----	5
5.2 Scope-----	5
5.3 General Acceptable Use Principles -----	5
5.4 Acceptable Use Requirements-----	6
5.5 Prohibited Activities-----	6
5.6 Compliance and Disciplinary Action-----	6
5.7 Policy Review-----	6
6. Information System and Services Usage-----	9
6.1 Information Usage -----	9
6.2 Email Usage-----	10
6.3 Intranet Usage -----	11
6.4 Internet Usage-----	12
6.5 Remote Access-----	12
6.6 Password Usage -----	13
6.7 Printer Usage -----	13
6.8 Data Transfer and Content Filtering -----	14
6.9 Telephone Usage-----	14
7. Posting Official Information On Websites-----	14
8. Posting Personal Information On Website-----	15
9. Socially Engineered / Fraudulent Mail-----	15
10. Compliance and Monitoring -----	16
11. Disclaimer -----	16
12. Enforcement -----	16
13. Reporting Acceptable Usage Violation-----	16
14. References-----	16

## 1. Purpose

The purpose of this policy is to outline the acceptable use of information systems and services provided by AIQUANT Technologies (Pvt) Ltd. ("AIQUANT") to its employees, temporary employees, and third-party contractors. AIQUANT users are required to read and formally accept the Acceptable Usage Policy before gaining access to AIQUANT information system and / or services.

## 2. Scope

The process included in this document applies to information processing facilities including information systems, applications and data centres included in the Information Security Management System (ISMS) scope and boundaries at AIQUANT.

## 3. Audience

The users of this document are all employees, contractors and third-parties of AIQUANT.

## 4. Definition

Term	Definition
Availability	Availability is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorised entity. Assets include things like information, systems, facilities, networks, and computers. All of these assets must be available to authorised entities when they need to access or use them.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Digital Data	Non tangible information assets
Information assets	Any information that has value to the organisation
Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, nonrepudiation and reliability can also be involved
Integrity	The property of safeguarding the accuracy and completeness of assets
Information Security Management System (ISMS)	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
Physical assets	Tangible information assets (paper documents, backup tapes etc.)
Phreaking	Phreaking is a slang term coined to describe the activity of a culture of people who study, experiment with, or explore, telecommunication systems, such as equipment and systems connected to public telephone networks.
TST	Technical Support Team, group or individual that are responsible for support and maintenance of the AIQUANT technical infrastructure
MC	Information Management Security Committee

## 5. Acceptable Use of Information Assets

### 1. Purpose

This policy defines the acceptable use of information assets to ensure the confidentiality, integrity, and availability of organizational information and to protect intellectual property, customer data, and systems from misuse, loss, or compromise.

### 2. Scope

This policy applies to all:

Employees, interns, and contractors

Information assets, including data, software, systems, networks, and devices

Physical and electronic information, whether stored, processed, or transmitted

### 3. General Acceptable Use Principles

Users shall:

Use information assets **only for authorized business purposes**

Access information **strictly on a need-to-know basis**

Comply with information classification and handling requirements

Protect credentials and authentication mechanisms

Follow all applicable legal, contractual, and regulatory requirements

### 4. Acceptable Use Requirements

#### 4.1 Use of Information

Access information only if required for assigned job responsibilities

Ensure information is used in accordance with its classification (Public, Internal, Confidential, Restricted)

Verify authorization before sharing information internally or externally

#### 4.2 Use of Systems and Applications

- Use only organization-approved systems, applications, and cloud services
- Follow secure development practices when handling source code and R&D artifacts
- Do not install unauthorized software or tools without approval

#### 4.3 Use of Credentials and Access Rights

- Maintain confidentiality of usernames, passwords, API keys, and cryptographic keys
- Use multi-factor authentication where enforced
- Do not share or reuse credentials
- Report suspected credential compromise immediately

#### **4.4 Use of Email, Messaging, and Collaboration Tools**

- Use official communication tools for business communication
- Avoid sharing Confidential or Restricted information via unsecured channels
- Validate recipients before sharing sensitive information
- Be vigilant against phishing and social engineering attempts

#### **4.5 Use of Endpoint Devices**

- Use organization-issued or approved devices for business work
- Ensure devices are protected with strong authentication and encryption
- Lock devices when unattended
- Do not store organizational data on unauthorized personal devices or removable media

#### **4.6 Remote Work and External Access**

- Use secure remote access mechanisms (VPN/MFA)
- Ensure home or remote work environments do not expose information to unauthorized persons
- Avoid using public or unsecured Wi-Fi for accessing sensitive systems

#### **4.7 Use of Source Code and R&D Assets**

- Access source code repositories only as authorized
- Do not copy, fork, or distribute proprietary code outside approved repositories
- Ensure open-source usage complies with licensing and organizational policies

### **5. Prohibited Activities**

Users shall **not**:

- Access, copy, modify, or delete information without authorization
- Share passwords, private keys, or security tokens
- Use information assets for personal, illegal, or unethical purposes
- Disable or bypass security controls
- Introduce malicious code or tools
- Upload organizational data to personal cloud storage or external platforms without approval

## **Incident Reporting**

Any suspected loss, misuse, unauthorized disclosure, or compromise of information assets must be reported immediately to the ISMS / Information Security team at [incidents@aiquantgroup.com](mailto:incidents@aiquantgroup.com).

Users shall cooperate during incident investigations.

## **6. Compliance and Disciplinary Action**

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract, and legal action where applicable.

Violations may be reported to relevant authorities if required.

## **7. Policy Review**

This policy shall be reviewed annually or upon significant changes to systems, business processes, or regulatory requirements.

# **6. Information Systems and Services Usage**

- All users shall take due care to protect AIQUANT IT systems and resources from unauthorised access, tampering and / or accidental damage.
- Logon banners must be configured to explicitly state conditions of access to a system, including:
  - access is restricted to authorised users
  - acceptable usage and information security policies
  - the user's agreement to abide by abovementioned policies
  - informing the user of activity monitoring and auditing
  - legal ramifications of violating the relevant policies
  - a point of contact for questions on these conditions.
- Legal advice shall be sought on the exact wording of logon banners.
- Logon banner text:
  - This is a AIQUANT Systems device and should only be accessed by an authorised AIQUANT employee or contractor in line with all AIQUANT policies and procedures. By continuing you agree to these policies and that anything you do with this device may be monitored and audited. Failure to comply can result in prosecution. For any questions contact IT.

- All AIQUANT information systems including desktops, laptops, mobile devices, printers, fax machines, photocopiers, as well as networks, servers and applications will only be used for their intended and authorised business purposes.
- Users shall not use AIQUANT provided facilities and services for illegal or unlawful purposes, including, but not limited to copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
- Users shall not use AIQUANT systems or networks to access unauthorised systems, networks and / or services.
- Users shall not install any software or applications which is not included within the AIQUANT Authorised Software List, into desktops or laptops given by AIQUANT for business purposes.
- Users with administrative rights shall not disable or by-pass any controls, such as anti-virus software, proxy servers and / or firewalls, implemented to protect AIQUANT network and / or information assets. Such by-pass shall be considered an information security violation and may lead to disciplinary actions according to Human Resources policies and procedures.
- Users with administrative rights shall not install unacceptable software, Network Scanning or Hacking tools on their devices unless authorised by AIQUANT.
- Users with administrative rights shall not install any software that does a similar function to a standard AIQUANT software like internet browsers, anti-virus or anti-spyware software.
- Users with administrative rights shall not install any pirated software.
- Each user of AIQUANT shall be provided with access to
  1. A OneDrive business account to store their business-related data;
  2. The company document repository in SharePoint.
  3. A common network shared storage space.The data / information contained within the provided locations are under the custody of the respective users. Users must not store unauthorised content in such folders.
- Sensitive or important content must not be stored in the common shared storage space and instead must be stored in OneDrive or SharePoint.
- Users must save their critical data to the appropriate location so that these data can be backed up regularly, in accordance with the AIQUANT backup policy, procedure and schedules.

## 6.1 Information Usage

- Users shall not disclose, communicate or discuss in public, any AIQUANT private, sensitive or confidential information.
- Users are expected not to store or transfer sensitive / confidential information using removable media.
- Users shall not post any AIQUANT related sensitive or confidential information on publicly accessible internet sites, such as mailing lists, public news groups or Skype / IM clients, without obtaining appropriate authorised approval.
- Users shall obtain appropriate intellectual property rights / copyright or contractual clearances before using any proprietary material. Using or providing AIQUANT developed software, innovative ideas, designs or repositories (software or otherwise) outside the AIQUANT environment is prohibited.
- Users shall use, handle and treat all information in accordance with the information asset management procedure.
- Users shall not transmit sensitive or confidential information, over the network, without adequate protection controls. All documents / excel sheets based on the information

classification (sensitivity) shall be password protected and any other information shall be zipped and password protected. Further passwords should be sent via a separate communication channel. E.g. Telephone. If an employee needs assistance in communicating sensitive or confidential information, he or she should contact the IS Officer.

- Before sharing any information about the AIQUANT information security environment, users shall confirm the identity and the need-to-know of the recipient. In the event the user is not able to confirm the identity and / or the need-to-know of the recipient, such requests should be forwarded to the MC.

## 6.2 E-mail Usage

- AIQUANT employees are encouraged to use email to promote the goals and objectives of AIQUANT as well as for fulfilling business and role-oriented tasks. AIQUANT employees are therefore expected to check their email in a consistent and timely manner so that they are aware of important company announcements and updates.
- All employees of AIQUANT are entitled to an email account. E-mail accounts will be granted to third party non-employees on a case-by-case basis with appropriate approval by the MC. Possible non-employees that may be eligible for email access include:
  - Contractors and
  - Vendors.
  - Email users are responsible for mailbox management, including organisation and cleaning.
- Email access at AIQUANT is controlled through individual accounts and passwords. It is the responsibility of the employee to protect the confidentiality of their account and password information.
- Users shall not use AIQUANT provided email facilities for illegal or unlawful purposes, including, but not limited to copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
- Users are not permitted to use any other user's email account without his / her approval.
- Use of personal and / or external email services for business messaging is prohibited, however MC's prior approval is required in cases where it is the only alternative method for email communication.
- Emails containing confidential or sensitive content must be protected in-line with the related information handling procedure, in electronic form, when printed onto paper or saved onto another media.
- Users will not open, execute or store emails and/or attachments received from unknown or un-trusted sources, and will report the presence of such emails or attachments to the TST.
- Users will use the organisation's standard email signature templates in all e-mail communications.
- Email access will be terminated when the employee or third party terminates their association with AIQUANT. AIQUANT is under no obligation to store or forward the contents of an individual's email inbox / outbox after the term of their employment has ceased.

## 6.3 Intranet Usage (Shared Portal / Network Locations)

- AIQUANT employees are encouraged to use the AIQUANT's SharePoint / network locations collectively referred to as the "Document Repositories" to collaborate with other employees and share files and documents.
- AIQUANT employees are granted access to sections of the Document Repositories based on their need-to-access and the least-privileges required performing their duties.
- Document Repositories access may be granted to third party non-employees on a case-by-case basis with appropriate approval by the MC. Such access will always be based on their need-to-access and the least-privileges required to perform their duties.
- The following activities on the AIQUANT Document Repositories is prohibited:
  - To upload, download, or distribute pornographic or sexually explicit material;
  - Violate any local or federal laws in any country the Document Repositories are used;
  - To invade or abuse the privacy of others;
  - Violate copyright or use intellectual material without permission;
  - To use the portal for financial or commercial gain; and
  - To degrade or disrupt AIQUANT networks and systems' performance.
- No user may use the Document Repositories functionality to deliberately propagate any Virus, Worm, Trojan horse, or trap door program code.
- Users are not permitted to use any other user's Document Repositories account without his / her approval.
- Documents containing confidential or sensitive content must be protected in-line with the related information handling procedure, in electronic form, when printed onto paper or saved onto another media.
- Users shall not store documents received from unknown or un-trusted sources and shall report the presence of such documents to the MC.
- Document Repositories access shall be terminated when the employee or third party terminates their association with AIQUANT.

## 6.4 Internet Usage

- Users must use AIQUANT internet services appropriately, responsibly and ethically.
- The internet access may not be used in a way that violates AIQUANT policies, rules or administrative orders.
- Users are restricted from using AIQUANT internet services on any illegal/offensive and/or related materials.
- Users shall not use AIQUANT internet services for illegal or unlawful purposes, including, but not limited to copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses). Any such activity may result in disciplinary action in-line with the Human Resources disciplinary policies and procedures.
- Users with administrative rights shall not alter or attempt to alter their internet access settings and / or configurations. Prior approval from the MC is required for cases where alteration is required for business purposes.
- Users are solely responsible for the content they disseminate or information they access through the internet services provided by AIQUANT.
- Users shall carefully read all security alerts presented by their internet web browser. If the user is unable to understand or is uncertain about the security alerts, he / she should contact the IS Helpdesk prior to proceeding with web browsing.

## 6.5 Remote Access

- It is the responsibility of any AIQUANT user with remote access privileges to ensure that their remote access connection remains as secure as possible.

- It is imperative that any remote access connection used to conduct AIQUANT business be utilised appropriately, responsibly, and ethically.
- Any AIQUANT user with remote access privileges shall not violate any of the AIQUANT Information Security Policies.
- Employees shall always use secure remote access procedures. This will be enforced through the use of strong passwords in accordance with the AIQUANT Acceptable Usage Policy's, password usage requirements.
- All remote computer equipment and devices used for business activity, whether personal or AIQUANT-owned, must implement reasonable physical security measures to avoid unauthorised access or misuse. Such computers shall have installed, appropriate antivirus software, deemed necessary by the MC.
- Any remote connection that is configured to access AIQUANT resources must adhere to AIQUANT Information Security policies, standards and guidelines.
- If AIQUANT-owned computer or related equipment used for remote access is damaged, lost or stolen, the respective user shall be responsible for immediately notifying the TST and the MC.
- The remote access user shall immediately report any incident or suspected incident of unauthorised access or disclosure of company resources, databases, networks or information.

## 6.6 Password Usage

- Users are reminded that they are personally responsible for all events that occur under their logon accounts. Therefore, users are responsible for keeping their passwords confidential.
- No employee is to give, tell, share or hint at their password to another person, including the IT staff, administrators, superiors, other co-workers, friends and family members, under any circumstances. If someone demands your password, refer them to this policy or have them contact the MC.
- It is advisable not to use "remember password" feature of applications such as internet browsers, email program or any other program.
- Passwords should not be transmitted electronically or any other means to any party internal or external to AIQUANT.
- If possible, users should use different passwords to access different systems.
- If an employee either knows or suspects that his / her password has been compromised, it must be reported to the MC and the password should be changed immediately.

## 6.7 Printer Usage

- AIQUANT printers should not be used to print personal documents.
- Installation of personal printers is generally not condoned at AIQUANT due to the cost of maintaining and supporting many dispersed devices. However, in certain circumstances, where confidentiality, remote location, the need to print a large number of low volume print jobs or other unusual circumstances warrants it, personal printers may be allowed with prior approval from the MC.
- Collect the printed copies as soon as it is printed. If the printed copy is no longer required, dispose it appropriately.
- Whenever possible please print documents in black and white.
- Make efforts to limit paper usage by taking advantage of duplex printing and other optimisation features.
- Avoid printing email messages. Instead use the folders and archiving functionality in the email application to organise and view messages.

- If you encounter a physical problem with the printer (paper jam, out of toner, etc.) and you are not trained to fix the problem, please do not attempt fixing the problem, instead, report the problem to the TST or ask a trained co-worker for help.
- Report malfunction of printers to the TST as soon as possible.

## 6.8 Data Transfer and Content Filtering

- Data transfer policies include requirements to ensure:
  - users are accountable for the data they transfer through AIQUANT's policies and procedures.
  - data transferred to a system of a lesser sensitivity or classification is approved by management
  - data imported to a system is scanned for malicious and active content and undergoes:
    - scanning for malicious and active content
    - data format checks
    - logging of each event
    - monitoring to detect overuse/unusual usage patterns
  - all data identified by a content filtering process as suspicious is blocked until reviewed and approved for transfer
  - antivirus scans are performed on all content using up-to-date engines and signatures
  - files that cannot be inspected are blocked and generate an alert or notification
  - the integrity of content is verified where applicable, and blocked if verification fails.

## 6.9 Telephone Usage

In many instances, voice networks and systems are subject to threats and vulnerabilities. "Phreakers" and other hackers use a variety of methods to eavesdrop on communications, causing denial of service attacks and expensive toll charges (toll fraud). To minimise the risk of these adverse events:

- Supervisors should ensure that deactivation requests are made in advance for accounts expected to be terminated in the foreseeable future
- Users shall not improperly access voicemail messages outside of their own individual account(s).
- Users shall not illegally intercept telecommunication signals or conversations.
- Access to switch and wiring closets shall be restricted to authorised individuals who require access to perform their job function.
- Each legitimate telephone end user shall set a PIN for their voicemail accounts and change regularly.
- Voicemail greetings shall not be recorded in such a way that will allow an operator to accept collect or third party billing telephone calls.

## 7. Posting Official Information on Websites

Personnel posting information on websites must maintain separate professional accounts from any personal accounts users have for websites.

## 8. Posting Personal Information on Websites

AIQUANT advises personnel to be aware that any personal information they post on websites could be used to develop a detailed profile of their lifestyle and hobbies in order to attempt to build a trust relationship with them or others. This relationship could then be used to attempt to elicit sensitive or classified information from them or implant malicious software on systems by having them, for example, open emails or visit websites with malicious content. See Socially

Engineered / Fraudulent Emails section for risks associated with posting personal information on websites.

- Personnel should minimise the amount of personal information posted on websites, avoiding where possible the following:
  - past and present employment details
  - personal details
  - schools/institutions
  - clubs/hobbies
  - educational qualifications
  - current work duties
  - work contact details.
- Personnel should use the privacy settings on websites to restrict access in situations where personal information is posted to only those they authorise to view it.

## 9. Socially Engineered / Fraudulent Emails

A scammer could contact a user pretending to be from a legitimate business such a bank, telephone or internet service provider. A user may be contacted by email, social media, phone call, or text message.

The following is a list of actions to be taken by all employees / contractors:

- Identify the real sender of the message (i.e. email)
  - View the email headers to see where the message really originated from
- Never click on links in emails
  - A common phishing technique is to include links in an email that look like they go to a legitimate website
  - Do an internet search using the names or exact wording of the email or message to check for any references to a scam – many scams can be identified this way
- Check whether the website is legitimate
  - A URL provided may appear to be legitimate, ensure that it is a trusted website and business. Most modern Internet Browsers will display the company name in green if the site has been issued an Extended Validation (EV) Certificate and is a legitimate website/business
- Some warning signs
  - The email or text message does not address a user by the proper name, and may contain typing errors and grammatical mistakes
  - The website address does not look like the address the user usually use and is requesting details the legitimate site does not normally ask for
  - Sender sent the message to an address that was not the one provided to the company
- Reporting scams
  - Users shall report scams or about suspicious mails to IT or seek advice from a senior employee.

## 10. Compliance and Monitoring

- Systems and services used / provided by AIQUANT are the property of AIQUANT. This gives AIQUANT the right to monitor all activities performed using these resources.

- Users shall maintain continued compliance with all AIQUANT policies, procedures, guidelines, rules and administrative orders while using AIQUANT systems, facilities and / or services.
- If AIQUANT discovers or has good reason to suspect activities that do not comply with applicable laws or policy, activity logs or records may be retrieved and used / presented as evidence for disciplinary action against the involved user.

## 11. Disclaimer

- AIQUANT assumes no liability for direct and / or indirect damages arising from a user's use of AIQUANT systems and / or services.
- Users are solely responsible for the content they disseminate or information they access.

## 12. Enforcement

- Any identified violation of this policy will first be assessed and subsequently discussed with HR and the employee. Based on the severity of the issue and the motivation that led to the violation, formal disciplinary actions may be taken resulting in any of the following outcomes
  1. First warning letter
  2. Final warning letter
  3. Termination of employment letter

## 13. Reporting Acceptable Usage Violations

- Violation of this policy or any other information security policy or procedure by another user, employee, contractor or third-party service provider should be reported to IT

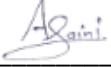
## 14. References

1. ISO/IEC 31000:2018 Information Technology – Security Techniques – Information Security Risk Management
2. ISO/IEC 27003:2022 Information Technology – Security Techniques – Information Security Management Systems Implementation Guidance
3. ISO/IEC 27001:2022 Information Security, Cyber Security and Privacy Protection – Information Security Management Systems – Requirements
4. ISO/IEC 27000:2022 Information Technology – Information Security, Cyber Security and Privacy Protection – Information Security Management Systems – Overview and Vocabulary
5. AIQUANT - ISMS-Scope
6. AIQUANT - Statement-of-Applicability

*I have read, understood and accepted all the contents and subjects explained hereinabove.*

Name: Asharam Sani

Place: Kolkata

Signature: 

Date: 31 Jan 2026