Quidlab Information Security Management Policy for E-Meeting & Voting System & Video Conferencing System

Table of Contents

Change Control

Version	Author	Approved By	Date	Remark
1.0.0	ISMS	MD	5th May 2020	Baseline document
1.0.1	ISMS	MD	1st Sept 2020	Changes in Privacy policy which added separately at end of this section. Making it clear distinction between data retention policy for customer provided data & portal user data collected by quidlab
1.0.2	ISMS	MD	5th Oct 2020	Added log retention details. Updated personal data items to include ID card, copy of ID card etc Simplified policy to understand data provided by customer & collected on behalf of customer and logs. Added ETDA within scope. Added password Policy Updated retention period
1.03	ISMS	MD	9th Oct 2020	Added detailed network & communication security policy information Added report handling
1.04	ISMS	MD	14th Oct 2020	Updated Access Control Policy
1.05	ISMS	MD	7th Jul 2021	Updated personal data items to include customer supplied data for condo AGMs and shareholder meetings
1.06	ISMS	MD	1st Sept 2021	Added, allow removal of personal data before 90 days on request
1.07	ISMS	MD	1st Sept 2021	Added Chanel of communication
1.08	ISMS	MD	6th Sept 2021	Updated Data encryption
1.09	ISMS	MD	8th Sept 2021	Updated: Record of Logs, Collecting and Using Your Personal Data and added Acceptable Use of the Service
1.10	ISMS	MD	26th May 2022	Data protection policy & terms of use made as separate document
1.11	ISMS	MD	18th Oct 2022	Added Cryptography methods for E2EE
1.12	ISMS	MD	6th June 2024	Added data backup Policy
1.13	ISMS	MD	18th Nov 2024	Added Safe Coding practices section

Objective

Provide customers with assurance that the E-Meeting & Voting system and Video Conferencing System provided by Quidlab shall be managed effectively, securely and responsibly.

Provide assurance that the customer's informational assets shall be protected against all internal, external, deliberate and accidental threats.

Where Quidlab installed systems necessarily interface with existing customer systems and networks this document shall provide additional assurance that the Quidlab system shall not adversely affect existing networks and systems and existing systems shall not adversely affect the Quidlab system.

Please note this plan does not fully detail what the customer should do to implement their own Information Security Management System. This plan details only the Quidlab owned systems and services that delivered and where those systems/people communicate with the systems at the customer site or utilize the informational assets of the customer.

This is a public document mandatory for all employees to read and comply. All customers, suppliers and other stakeholders are encouraged to read.

Purpose

Confidentiality:

Ensuring that information is accessible only to those authorized to have access

Integrity:

Safeguarding the accuracy and completeness of information

Availability:

Ensuring that authorized users have access to information when required

Security & Data protection Policy

- Management's commitment to support the policy
- Management shall ensure documented procedures are provided as far as possible. Procedures which are not documented are accepted if communicated to employees in form of training and proof of training is maintained and documented.
- The Policy ensures that
  - Asset Management is maintained

  - Access control procedures are followed
  - Data encryption procedures are followed
  - Creating physical and environmental security
  - Information shall be protected against unauthorized access
  - Confidentiality of information shall be assured
  - Integrity of information shall be maintained
  - Availability of information for business processes shall be maintained
  - Legislative and regulatory requirements shall be met
  - Business continuity plans shall be developed, maintained and tested
  - Informational security training shall be available for all employees
  - All actual or suspected information security breaches shall be reported to the management and shall be thoroughly investigated.
- Business requirements for availability of information and systems shall be met
- Company Authorized person is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the information security policy is mandatory.

Scope

Scope of this policy covers Quidlab E-Meeting & Voting System and Quidlab Video Conference System including future modules pertaining to E-Meeting & Video Conferencing only. This policy is prepared meeting guidelines for E-meeting System from Electronic Transactions Development Agency (ETDA) & ISO 27001 standards.

Chanel of communication (Added 1st Sept 2021)

This policy is available on Quidlab website, login page of FoQus portal and link to this policy is also included to attendees' invitation emails.

Overview

Quidlab E-Meeting & Voting System and Quidlab Video Conference System are presently provided two different offerings as Software as Service (SAAS). Quidlab E-Meeting & Voting System is main offering specially designed for shareholders meetings where as Quidlab Video Conference System can be used for general E-meetings.

Security Management & Data Protection Policies

Management ensures security management procedures are developed, communicated and understood by all relevant employees. Procedures can be in form of written manuals, trainings and other management communication e.g. by email.

These procedures must include at least following:

Asset Management Policy

In managing the assets belonging to Quidlab, we are committed to maintain procedures & records of:

- Inventory of Assets
- Ownership of Assets
- Acceptable Use of Assets
- Return of Assets
- Classification of Information including personal data
- Handling of Assets
- Management of Removable Media
- Disposal of Media
- Physical Media Transfer

Access control Policy (Updated 14th Oct 2020)

Access control policy has been established, documented, and periodically reviewed on the basis of business and security requirements.

Access control rules and rights for each user or group of users are clearly stated in the access control policy.

Our access control policy has taken account of the following:

a) security requirements of individual business applications

b) identification of all information related to the business applications and the risks the information is facing

c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information

d) consistency between the access control and information classification policies of different systems and networks

e) relevant legislation and any contractual obligations regarding protection of access to data or services

f) standard user access profiles for common job roles in the organization

g) management of access rights in a distributed and networked environment which recognizes all types of connections available

h) segregation of access control roles, e.g. access request, access authorization, access administration

i) requirements for formal authorization of access requests

j) requirements for periodic review of access controls, and

k) removal of access rights.

In managing the Access Control we are committed to maintain procedures & records of:

- Access to Networks and Network Services
  Users would only be provided with access to the network and network services that they have been specifically authorized to use.
- User Registration and Deregistration
- A single service/system account should not be shared or used across multiple services to avoid excessive privileges that could lead to security risks. Each service or system should have a unique account with minimal permissions necessary to perform its specific function, following the principle of least privilege. This approach limits the potential damage in case of credential compromise and ensures better accountability by enabling detailed activity tracking per account. Additionally, service accounts should be monitored regularly, with strict access control policies, periodic password rotations, and the use of secure secrets management solutions to further enhance security.

Formal procedure for user registration and de-registration are in place to enable assignment of access rights. It also covers a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services.

- **User Access Provisioning**
  The access control procedure for user registration & de-registration and user access provisioning includes:

  a) Using unique user IDs to enable users to be linked to and held responsible for their actions; the use of group IDs are permitted only where they are necessary for business or operational reasons, and must be approved and documented
  b) Checking that the user has authorization from the system owner for the use of the information system or service
  c) Checking that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy
  d) Giving users a written statement of their access rights
  e) Requiring users to sign statements indicating that they understand the conditions of access
  f) Ensuring service providers do not provide access until authorization procedures have been completed
  g) Maintaining a formal record of all persons registered to use the service
  h) Immediately removing or blocking access rights of users who have changed roles or jobs or left the organization
  i) Periodically checking for, and removing or blocking, redundant user IDs and accounts, and
  j) Ensuring that redundant user IDs are not issued to other users.

- **Management of Privileged Access Rights**
  a) The access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated have been identified.

b) Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy, i.e. the minimum requirement for their functional role only when needed.
c) Authorization process and a record of all privileges allocated is maintained. Privileges are not granted until the authorization process is complete.
d) The development and use of system routines has been promoted to avoid the need to grant privileges to users.
e) The development and use of programs which avoid the need to run with privileges are being promoted.
f) Privileges are assigned to a different user ID from those used for normal business use.

- **Management of Secret Authentication Information of Users**
  a) Users are required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group. This signed statement is included in the terms and conditions of employment.

  b) When users are required to maintain their own passwords they are provided initially with a secure temporary password, which they are forced to change immediately.

  c) The identity of a user is verified (by sending a secret code to the user's official email ID and asking him / her to confirm the secret code) prior to providing a new, replacement or temporary password.

  d) Temporary passwords are given to users in a secure manner (such as sending via SMS to his / her mobile phone). The use of third parties or unprotected (clear text) electronic mail messages is avoided.

  e) Temporary passwords would be unique to an individual and are not guessable.

  f) Users need to acknowledge receipt of passwords, by email or reply SMS.

  g) Passwords are never be stored on computer systems in an unprotected form. They are always masked / encrypted and stored.

  h) Default vendor passwords are altered following installation of systems or software.

- **Review of User Access Rights**
  a) Users' access rights are reviewed at regular intervals; and also after any changes, such as promotion, demotion, or termination of employment.
  b) User access rights are reviewed and re-allocated when moving from one employment to another within the same organization.
  c) Authorizations for special privileged access rights are reviewed at more frequent intervals (3 months).
  d) Privilege allocations are checked at regular intervals (6 months) to ensure that unauthorized privileges have not been obtained.
  e) Changes to privileged accounts are logged for periodic review.

- **Removal or Adjustment of Access Rights**
  The access rights of all employees and external party users to information and information processing facilities would be removed upon termination of their employment, contract or agreement, or adjusted upon change.

User Manuals and Password Management Guidelines Policy

The company has a clear policy to provide user manuals and guidelines to ensure employees and users can effectively and securely utilize its systems and services. These manuals include detailed instructions on system usage, account setup, and the steps to change passwords regularly. The policy emphasizes the importance of creating strong, unique passwords and provides tips on secure password management. By offering these resources, the company aims to enhance user awareness, minimize security risks, and promote compliance with organizational security standards. Regular updates to the manuals are provided to reflect changes in systems, ensuring users have access to the most accurate and up-to-date information.

Data encryption (Updated 18th Oct 2022)

Data encryption covers FoQus E-meeting system data and personal information provided directly or indirectly to us as defined under section 'Collecting and Using Your Personal Data'.

In managing the Data encryption we are committed to maintain procedures & records of:

- Data is encrypted at rest and in transit
- Data is encrypted End-to-End
- Audio & Video streams are encrypted using DTLS-SRTP protocols (with AEAD_AES_256_GCM encryption). For E2EE additional protection is applied End to End and support is made for browsers which can support insertable streams.

Quidlab does not allows use of removable media eg. USB on computers used for FoQus E-meeting system. All reports to customer are sent by email, which are encrypted in transit and at rest.

Creating physical and environmental security

In managing the Physical and environmental security we are committed to maintain procedures & records of:

- Creating physical and environmental security procedures must include at least
- Creating Physical Security Perimeter
- Physical Entry Controls
- Protecting against External & Environmental Threats
- Working in Secure Areas
- Delivery & Loading Areas

Operations Security

In managing the Operational security we are committed to maintain procedures & records of:

- Documented Operating Procedures or documented training sessions
- Change Management
- Capacity Management
- Separation of Development, Testing & Operational Environments
- Production environments are not allowed to access by users & developers of testing and development environments

- Any changes to application shall be tested prior to production and tested for no other impact on other services

Security for data communication (updated 9th Oct 2020)

In managing the Security for data communication we are committed to maintain procedures & records of:

- Security of non-electronic data communication
- Security of electronic data communication

Network Security Management & Network controls

Networks (Local Area Network) are adequately managed and controlled to protect information in systems and applications. Network managers have implemented controls to ensure the security of information in networks, and the protection of connected services from unauthorized access.

The following items have been taken care of:

a) Operational responsibility for networks has been separated from computer operations where appropriate

b) Responsibilities and procedures for the management of remote equipment, including equipment in user areas, has been established

c) Special controls are established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems & applications, and to maintain the availability of the network services and computers connected

d) Appropriate logging and monitoring is applied to enable recording of security relevant actions, and

e) Management activities are closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information-processing infrastructure.

f) All ports and services including insecure services and protocols which are not required are disabled and allowed services must use version TLS 1.2.

Security of network services

Network services include the provision of connections, private network services, and value-added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a) Technology applied for security of network services, such as authentication, encryption, and network connection controls

b) Technical parameters required for secured connection with the network services in accordance with the security and network connection rules, and

c) Procedures for the network service usage to restrict access to network services or applications, where necessary.

The ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored, and the right to audit has been agreed upon.

Security mechanisms, service levels and management requirements of all network services have been identified and included in the network services agreements, whether these services are provided in-house or outsourced.

The organization would ensure that network service providers implement these measures.

Segregation in networks

Groups of information services, users, and information systems are appropriately segregated on networks.

Quidlab will also maintain network security controls to ensure the protection of information including personal information within its networks, and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information of electronic data communication. Quidlab will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems including use of Email – blocking potential harmful content and attachments, using encryption for data in transit and at rest, Email authenticity eg. SPF records, firewalls, segregation of networks, remote access polices etc. Network and information communication will be controlled by roles & rights of users.

Information Security Incident Management (updated 5th Oct 2020)

In managing the Information Security Incident Management we are committed to maintain procedures & records of:

- Responsibilities & Procedures
- Reporting Information Security Events
- Reporting Information Security Weaknesses

- Assessment of & Decision on Information Security Events
- Response to Information Security Incidents
- Learning from Information Security Incidents
- Collection of Evidence

Security Incidents discovered by all stakeholders can be reported via email to info@quidlab.com, however employees can also follow Whistleblower reporting channel as covered under this policy.

Information Security Aspects of Business Continuity Management

In managing the Information Security Aspects of Business Continuity Management we are committed to maintain procedures & records of:

- Planning Information Security Continuity
- Implementing Information Security Continuity
- Verify, Review & Evaluate Information Security Continuity

Information Security Risk management

In managing the Information Security Risk management we are committed to maintain procedures & records of:

- Identifying Risks
- addressing risks and opportunities
- Information security risk treatment

Management Review Policy

Our Management Review Policy requires:

- Review Policy & Procedures at least one per year & change if required
- Review Policy & procedures whenever there are significant changes to regulations & laws or standards within scope of policy

Data retention Policy (updated 1st Sept 2020)

Our policy is to destroy all personal confidential e-meeting data provided by customers after 90 days of meeting and when all reports are handed over to meeting organizer, Organizer may request us to keep data for a longer period upon written request. Organizer may request personal data removal in writing before 90 days if such removal is in line with laws.

Data backup Policy (Updated 6th Jun 2024)

Data is backed up at regular intervals and can be restored. Backups are also deleted when data retention time expires after 90 days.

Record of Logs (Added 5th Oct 2020)

Company keeps various records of logs eg application logs, event logs, user access logs. Some logs are required by laws (e.g. Computer Crime Act B.E. 2550 and the Personal Data Protection Act B.E. 2562, STANDARDS FOR MAINTAINING SECURITY OF MEETINGS VIA ELECTRONIC MEANS B.E. 2563 (2020) etc.

Thailand Computer Crime Act B.E. 2550 requires access logs to be maintained for at least 90 days. To simplify procedures and avoid confusion company has set a policy to keep records of all logs for minimum 90 days. However, any logs which can identify personal information are deleted after 90 days. IP address if not linked to other personal data is not considered as personal data.

Password Policy (Added 5th Oct 2020)

Quidlab's policy ensures the use of strong security practices in the selection, storage, and management of passwords. Passwords must be stored securely in databases or configuration files using strong encryption methods like AES-256 or hashing algorithms such as SHA-256 with salts. During the first login, users are required to change their passwords to prevent unauthorized access. The policy enforces account lockout after a defined number of incorrect login attempts to protect against brute force attacks. Additionally, passwords must adhere to strong criteria, including a minimum length of 8 characters, the use of a mix of upper and lowercase letters (A-Z, a-z), numbers (0-9), and special symbols (*, #, %, etc.). Passwords must also be updated periodically, and the reuse of previous passwords is prohibited. These practices ensure robust protection of user accounts and safeguard organizational systems against potential threats.

User accounts and passwords for non-production environments shall conform the same standards as on production environments and are not same for production, testing & development. Furthermore, for every new customer tenant, passwords must be reset upon creation and must not be the same as passwords for other customers, ensuring unique and secure credentials for each tenant. Every customer should also have separate cryptographic key and certificates.

Policy on Server Certificates

All server and WebApp certificates used must be issued by a trusted and reputable Certificate Authority (CA) to ensure the authenticity, integrity, and confidentiality of communications. Self-signed certificates are strictly prohibited as they do not provide the necessary trust validation and pose security risks.

The organization mandates the use of certificates that comply with industry standards for encryption (e.g., TLS 1.2 or higher). Certificates must be renewed before expiration to maintain secure operations. All issued certificates must be tracked in an inventory, and periodic audits must be conducted to ensure compliance with this policy.

By using CA-issued certificates, the organization guarantees secure connections, protects sensitive data during transmission, and prevents vulnerabilities associated with untrusted certificates.

Safe Coding Practices (Added 18th Nov 2024)

The Safe Coding Practices Policy ensures secure software development by following industry best practices like OWASP Top 10 and secure coding standards. All user inputs must be validated to prevent injection attacks, and sensitive data must be securely stored and transmitted using encryption. Strong authentication and authorization controls, such as MFA and role-based access, must be enforced, and credentials should never be hardcoded in source code—secure vaults or environment variables must be used instead. Proper error handling should prevent information leakage, and third-party dependencies must be regularly updated and sourced from trusted repositories. Security-focused code reviews and testing (SAST, DAST) are mandatory before deployment. Applications must use security headers (e.g., CSP, HSTS) and follow secure configurations by disabling unnecessary services. Logging must capture security events without exposing sensitive data, and logs should be reviewed for suspicious activities. Non-compliance with these practices may result in corrective actions as per the ISMS framework.

Server Hardening Policy

All infrastructure components, including operating systems, databases, and middleware, must be hardened before going live, after major updates, and at regular intervals based on security best practices. Hardening shall follow industry standards such as CIS Benchmarks, NIST, and Azure Security Best Practices. For cloud-based PaaS applications, a server hardening report must be generated and reviewed upon significant changes to ensure compliance with organizational security requirements.

Vulnerability Assessment Policy (Added 5th Oct 2020)

The purpose of this policy is to grant authorization to appropriate members of the Information Security Team to conduct audits, consisting of vulnerability assessments and penetration tests, against the Quidlab FoQus E-meeting system.

The Information Security Team will run periodic, vulnerability scans at least once in 12 months or whenever a significant code changes are made to FoQus system. Results of these scans will be addressed in accordance with the risk posed. The Information Security Team will use the Common Vulnerability Scoring System (CVSS) to aid in setting patching guidelines.

All stakeholders are encouraged to notify any bugs or vulnerabilities found by email to info@quidlab.com

Whistleblower Policy (Added 5th Oct 2020)

A whistleblower as defined by this policy is an employee of (Quidlab Co., Ltd.) who reports an activity that he/she considers to be illegal or dishonest to one or more of the parties specified in this Policy. The whistleblower is not responsible for investigating the activity or for determining fault or corrective measures; appropriate management officials are charged with these responsibilities.

If an employee has knowledge of or a concern of illegal or dishonest fraudulent activity, the employee is to contact his/her immediate supervisor. The employee must exercise sound judgment to avoid baseless allegations. An employee who intentionally files a false report of wrongdoing will be subject to discipline up to and including termination.

Whistleblower protections are provided in two important areas - confidentiality and against retaliation. Insofar as possible, the confidentiality of the whistleblower will be maintained. However, identity may have to be disclosed to conduct a thorough investigation, to comply with the law and to provide accused individuals their legal rights of defense. The Company will not retaliate against a whistleblower. This includes, but is not limited to, protection from retaliation in the form of an adverse employment action such as termination, compensation decreases, or poor work assignments and threats of physical harm. Any whistleblower who believes he/she is being retaliated against must contact Managing Director immediately. The right of a whistleblower for protection against retaliation does not include immunity for any personal wrongdoing that is alleged and investigated.

All reports of illegal and dishonest activities will be promptly submitted to the Managing Director who is responsible for investigating and coordinating corrective action.

Employees with any questions regarding this policy should contact their Supervisor.