QTERMINALS

IT SECURITY POLICY

Contents

1. PURPOSE AND POLICY STATEMENT

QTerminals recognises the importance of the information that we hold on behalf of its customers, stakeholders, and Employees. Accordingly, we are committed to secure all information while it is being handled, processed, stored, transmitted, and delivered through safe, responsible, and secure IT systems and practices.

This IT Security Policy (hereinafter “Policy”) aims to provide general guidance on IT security and protection of Company’s information in a simple and concise manner. More detailed guidance and instructions are provided in Information Security Management System (ISMS) Policy Manual, which also outlines applicable key procedures, roles, and responsibilities. Therefore, both Policy and ISMS Policy Manual should be treated as complimentary as they do not replace or override one another.

2. SCOPE OF APPLICATION

The Policy applies globally to all Employees. This Policy does not replace any national or international law. In case of any conflict, legislation must take precedence over this Policy. Employees are requested to promptly notify IT team in case such conflict is identified.

3. DEFINITIONS

Employees means all employees (including contracted workers), officers and directors of QTerminals.

Ethics Review Panel (ERP) means a multidisciplinary body within QTerminals committed to reviewing all reported alleged unethical matters, misconduct and wrongdoings in a timely manner and deciding on the respective disciplinary action. ERP members are selected on a case-by-case basis by the Group Legal and Compliance Director, depending on the nature and criticality of the alleged misconduct and/or wrongdoing.

Line Manager is a person with direct managerial responsibility for a particular Employee.

QTerminals or Company means QTerminals W.L.L. and its controlled subsidiaries, affiliates, and joint ventures.

4. IT SECURITY GUIDELINES

1. Take good care of Company equipment

Employees are responsible for Company’s assets used while completing their tasks (e.g., printers) and personal equipment provided by the Company (e.g., smartphones, laptops). To take good care of Company’s equipment, **Employees should**:

- Operate and maintain equipment according to manufacturer’s specifications and exercise care in protecting such devices against loss, theft, damage, or destruction. Employees will be held responsible in case of failures, breakdowns, damages that are deemed due to negligence or deliberate misconduct by the respective Employees.
- Contact the IT Help Desk in case of failure or breakdown of the equipment and IT Department will proceed to its reparation.
- Obtain approval of Line Manager and IT Director to receive individual equipment outside of typical equipment for Employees position or bespoke configurations of the equipment.

In relation to Company's equipment, **Employees are prohibited** from:

- Using QTerminals' IT facilities and resources in connection with the operations or management of any business other than that of QTerminals.
- Reallocating equipment to another Employee. Only IT Department has the discretion to allocate and reallocate equipment.
- Tampering with the Company equipment or its software (e.g., deactivating or modifying the anti-virus software).
- Removing devices such as desktops, printers, scanners from QTerminals premises. Removal of these devices in exceptional cases requires a specific written approval by Information Security Officer, Data Owner, and Administrator. This is not applicable to devices that are by nature mobile, namely laptops, tablets, and smartphones, and these may be freely moved by Employees to and from QTerminals premises.

In case you need further information about protection of Company's assets, please refer to Chapter 10 of ISMS Policy Manual. If ISMS Policy Manual does not provide answer to your question, please reach out to IT Help desk of your business unit.

2. Classify all data and protect sensitive data

Protecting sensitive data is multi-step process that at first requires critical evaluation and classification based on its confidentiality, integrity, and availability. To ensure protection of sensitive data, **Employees should**:

- Mark all assets, emails, records, and media containing sensitive information with words "CONFIDENTIAL", "INTERNAL" or "RESTRICTED" according to Information Classification Policy. Respective markings should be put in prominent places, such as headers, title pages, stamps, labels, etc. to ensure clear visibility.
- Protect all non-public information from unauthorised access and eavesdropping.
- Lock away all non-public information and lock or log off from the equipment when Employee's desk is unattended.
- Configure all devices to an automatic screen locking after a short period of inactivity.
- Use secure messaging (e.g., with encryption) to electronically transmit confidential information (grade C3).
- Ensure that Non-Disclosure Agreement (NDA) has been signed prior to exchanging sensitive information with a third party.

In relation to protection of sensitive data, E**mployees are prohibited** from:

- Using portable storage devices (e.g. USB sticks, external disk drives, SD cards due to their vulnerability to loss, theft, viruses, and malware) unless approved by the Line Manager and IT Director.
- Seeking access to data they know or ought to know is private or confidential, including accessing or viewing without permission any files stored on local hard disk of other Employees.
- Using cloud services to store or share Company-related information unless approved by the Line Manager and IT Director.

In case you need further information about information classification, please refer to Chapters 9, 13 and 14 of ISMS Policy Manual. If ISMS Policy Manual does not provide answer to your question, please reach out to IT Help desk of your business unit.

3. Use Internet and Intranet considerately

While Internet is essential for completion of daily tasks of QTerminals Employees, its misuse carries significant risks. Therefore, **Employees should**:

- Ensure that Internet activities do not negatively influence the Company or associate it with controversial issues. This is critically important because information identifying the Employee's PC may be logged when visiting a website. Therefore, any unauthorised and/or inappropriate activity of an Employee using the QTerminals' network may affect QTerminals and its reputation.
- Contact the IT Help desk for assistance in case one has a business need to access certain websites that are blocked by the IT Department of QTerminals.
- Keep in mind that QTerminals recognises the need for individuals to carry out some personal tasks during working hours, e.g., for internet banking or on-line shopping. However, this is permitted assuming personal tasks do not take priority over work responsibilities and do not have a negative impact on QTerminals in any way.

In relation to the use of Internet, **Employees are prohibited** from:

- Using organisational Internet or Intranet for undue personal gain.
- Using organisation Internet to download personal files of large size if it affects internet connection of other Employees.
- Visiting websites containing inappropriate content or downloading such content. Inappropriate content is anything that is considered illegal and improper e.g., cybercrime, cyber-bullying, or pornographic content.
- Using or downloading any material that is protected by copyright in violation of the terms of the licensing (e.g., pirated software or data).
- Registering or commenting at viewing message boards and web logs (blogs) using QTerminals' email address. Such resources can only be accessed in read only format, where no interactive log in is required for access.

In case you need further information about considerate use of Internet and Intranet, please refer to Chapter 16 of ISMS Policy Manual. If ISMS Policy Manual does not provide answer to your question, please reach out to IT Help desk of your business unit.

4. Use emails professionally and securely

To ensure appropriate use of email and protection of Company's information, **Employees should**:

- Use professional and respectful language in emails.
- Apply common sense when assessing whether email is legitimate because this communication channel is not fully secure, and its content could be altered during transmission.
- Verify all recipients of an email before sending to make sure that list contains appropriate recipients.
- Exercise care when using distribution list configured on the Company email system.
- Exercise care when deleting emails because they are difficult to recover. Although old emails are stored on the backup system, this is done for archiving and audit purposes and not for recovery considerations.
- Use alternative solutions to send attachments that exceed size limit, such as QTerminals One Drive links, compressing the large files, or sending separate smaller attachments.
- Keep in mind that Company provided e-mail address belongs to QTerminals and is provided purely for the purpose of conducting business. Occasional use for personal emails can be tolerated as long as personal emails: (a) do not interfere with the performance of professional duties, (b) do not take priority over work responsibilities, (c) do not cause unwarranted expense or liability to be incurred by QTerminals, (d) do not have a negative impact on QTerminals in any way.

In relation to the use of emails, **Employees are prohibited** from:

- Using foul and/or obscene language as well as using misleading content, spam, or chain e-mails.
- Using personal email for work purposes.
- Using "BCC" function for internal emails between QTerminals Employees.

- Opening emails received from suspicious email addresses, containing suspicious content or content received from unrecognised individuals or organisations due to the security risks inherent to external emails. In case where these emails contain attachments, do not open them. Instead, notify the IT Help Desk for further advice.
- Providing QTerminals e-mail address when using public web sites for non-business purposes, such as on-line shopping.
- Reading emails of another Employee without permission. Provision of calendar access rights by manager to their assistant is an exception and requires explicit authorisation of the manager.
- Sending emails of customers, vendors, stakeholders to their personal emails (e.g., Gmail), even if requested.

In case you need further information about email security, please refer to Chapter 17 of ISMS Policy Manual. If ISMS Policy Manual does not provide answer to your question, please reach out to IT Help desk of your business unit

5. Beware of IT security threats

Malware, social engineering and use of non-licensed software are among most significant threats to IT security systems. To prevent risks of unauthorised access to QTerminals' data, **Employees should**:

- Use only licensed and approved software on Company's equipment.
- Scan for viruses before using downloaded files from any source, including USB hard disks, network files, email attachments and files from the Internet.
- Be cautious of social engineering, psychological manipulations used by some hackers to gain access to critical information within the Company (e.g., via baiting, also known as false promise).
- Obtain approval from Line Manager and the IT Director for installation of any non-standard software (e.g., AutoCAD, Bloomberg).

In relation to IT security threats, **Employees are prohibited** from:

- Sharing any sensitive information in relation to QTerminals IT system such as passwords in any written or verbal form to anyone outside the Company.
- Downloading, installing, or using unauthorised software programs. Software that permits computers to be remotely controlled as well as packet-sniffing, password-detecting and other hacking tools are explicitly prohibited.
- Executing programs of unknown origin.
- Carrying out any hacking activities against QTerminals' systems or any external systems using QTerminals IT resources.
- Knowingly introducing:
  - any form of computer virus, worm, trojan horse or trap-door program code.
  - any devices or programs designed to overload any computer, server or network component, disable them or create attacks such as denial of service.
  - any devices or programs designed to circumvent any system intended to protect the privacy or security of Employees and data.

In case you need further information about software installation, please refer to Chapters 18, 20 and 27 of ISMS Policy Manual. If ISMS Policy Manual does not provide answer to your question, please reach out to IT Help desk of your business unit.

6. Choose secure passwords

When neglected, passwords can become a vulnerable element of the IT security system. To mitigate risks of unauthorised access to Company's data, **Employees should**:

- Change password immediately after the first-time login.

- Change password regularly (at least every 42 days).
- Select password that contains minimum 8 characters and at least 1 special character, number, capital, and small letters.
- Choose dedicated password for QTerminals devices that is not used anywhere else (e.g., for personal email, social media accounts, etc.).

In relation to passwords, **Employees are prohibited** from:

- Disclosing password to anyone except for authorised QTerminals IT team (for technical support purposes). If disclosed to IT team, password should be changed immediately after the IT issue is solved.
- Using generic or shared passwords unless specifically authorised by the IT team.
- Writing down passwords in plain text (unencrypted).

In case you need further information about password policy, please refer to Chapter 25 of ISMS Policy Manual. If ISMS Policy Manual does not provide answer to your question, please reach out to IT Help desk of your business unit.

7. Use approved messaging and video conferencing tools

Employees should use Microsoft Teams for messaging and video conferencing. Microsoft Teams is deployed on each desktop, laptop and can be deployed on the mobile phones of Employees of your business unit.

In relation to messaging, **Employees are prohibited** from:

- Using social networks or personal instant messaging software such as WhatsApp to exchange business-related information or documents due to inherent security risks involved.
- Using QTerminals email to register on a social network or posting any information about QTerminals and its business. The Corporate Communication Department is the sole department in charge of managing QTerminals' presence on social networks.

In case you need further information about use of messaging at QTerminals, please reach out to IT Help desk.

8. Protect Company's information while working from home

In order to facilitate work, the IT Department may grant Employees with VPN accounts that allow accessing QTerminals IT systems remotely, as required by role duties. **Employees should** prevent access to any QTerminals IT system or data by any non-authorised person when accessing QTerminals network from a personal computer.

In relation to working from home, **Employees are prohibited** from:

- Using public Wi-Fi networks without VPN connection.
- Accessing QTerminals IT systems from public computers.
- Communicating personal VPN account details to another Employee or a third party.
- Printing materials at any public computer.

In case you need further information about working from home policy, please reach out to IT Help desk of your business unit.

9. Obtain approval before using personal devices

To use personal devices for work-related purposes, **Employees should**:

- Keep in mind that only mobile devices or tablets owned by Employees can be configured and connected to QTerminals email system and Microsoft Teams collaboration tool. Other equipment purchased directly by the Employee cannot be configured or connected to QTerminals IT systems due to security risks.

- Refer to IT team for approval and support with configuration.
- Read and sign respective QTerminals policies before using personally owned laptop, smartphone, or tablet to access Company's resources.

In case you need further information about use of personal devices, please refer to Chapter 22 of ISMS Policy Manual. If ISMS Policy Manual does not provide answer to your question, please reach out to IT Help desk of your business unit.

10. Reach out to IT team if you notice a vulnerability

Employees should proactively ensure that the IT system of QTerminals is secure by immediately reporting to the IT team in case any of the following is observed:

- Unauthorised access or change to data.
- Malicious software/viruses.
- Inappropriate use of IT resources.
- Suspicious, unusual, or questionable activities.
- Any other weakness that compromises IT security of QTerminals.

In case you need further information about incident management, please refer to Chapter 33 of ISMS Policy Manual. If ISMS Policy Manual does not provide answer to your question, please reach out to IT Help desk of your business unit.

5. ACCESS TO EMPLOYEES' DATA

QTerminals is ultimately responsible for data residing on its IT systems (including PCs, laptops, tablets and smartphones) and is committed to comply with applicable legislation in relation to data protection. Accordingly, QTerminals can access Employee's data and communications for the following reasons:

- Providing evidence for police investigations.
- Ensuring laws and regulations are respected.
- Ensuring QTerminals internal procedures, policies and contracts are respected.
- Complying with legal and regulatory obligations.
- Investigating and preventing unlawful activities or unauthorised use of QTerminals systems.

To ensure Company's IT security, IT Department may access and monitor the following data relating Employees without their prior consent:

- Potentially harmful emails blocked by virus/antispam software (including unsolicited marketing e-mails (spam) and e-mails with potentially abnormal attachments). IT Department requires access in order to process and delete such emails in case they contain viruses.
- Internet traffic data and surfing (including the domain names, websites visited, duration of visits, non-business files downloaded from the internet and their size). Any abnormal surfing or violations would be reported to the IT Director for further action.
- Access logs to central systems (such as ERP, TOS, etc.). Any abnormal behaviour is reported to the IT Director.
- VPN access logs. Any abnormal behaviour is reported to the IT Director.

The IT Department does not monitor other communications or data of the Employees unless the consent of the Employee is obtained or if a police investigation is involved. However, this general rule may not apply under the following circumstances:

• In cases of Employee's absence (due to sickness, leave, death or any other reason) and unavailability using reasonable means (such as phone) upon instruction of QTerminals Group Diversity Director, Group IT Director, and Group Legal and Compliance Director.
• In cases of serious suspicion about unlawful activities being conducted using QTerminals' assets upon approval of Group Legal and Compliance Director.
• In cases of Employee's departure from the Company for the purpose of business and operations continuity. Access to relevant emails and documents may be provided to the Employee taking over their role whilst maintaining private messages and data as confidential.

6. RESPONSIBILITIES

All Employees are responsible for adhering to this Policy. We expect Employees to read, understand, acknowledge, and adhere to all aspects of this Policy and supplementary policies and procedures issued by QTerminals, including ISMS Policy Manual. All Employees are encouraged to contact the IT Help desk of their business units to clarify questions, request information or express concerns. Line Managers, along with the relevant guidance of IT department, shall ensure the addressing of concerns related to IT security from Employees.

Management is responsible for ensuring that the necessary means, resources and personnel needed to enforce this Policy are available. Each managing senior executive of QTerminals at port or terminal level must ensure that the business unit they are responsible for is and will remain fully compliant with this Policy, promoting awareness and understanding of this Policy and ensuring allocation of adequate resources to effectively implement this Policy. Specifically, the IT team must ensure that the required processes are in place that enable adherence to this Policy.

7. SPEAK UP

QTerminals promotes an environment of integrity and transparency under which its Employees are encouraged to report any violation or suspected violation of this Policy within QTerminals or at any of the third parties, either by informing their Line Manager, their HR department, their Compliance Officer/Representative or alternatively through the QTerminals Ethics Line, which is available on QTerminals intranet, QTerminals website and as a dedicated phone line.

Additionally, any retaliation against anyone who notices and reports a known or suspected violation of the Policy is strictly prohibited. Anyone proven to have retaliated against a person who has reported a breach in good faith is to be subjected to disciplinary action. However, any false or malicious allegations may lead to appropriate disciplinary and legal action, up to and including termination of employment.

For more information on the whistleblowing process, please refer to **QTerminals Whistleblower and Anti-fraud Procedures**.

8. DISCIPLINARY ACTION

At QTerminals, all to whom this Policy applies, as specified in the "Scope of Application" are expected to abide by this Policy. Any violation thereof may result in disciplinary action, termination of employment or legal proceedings.

In case the complaints for wrongdoings warrant an investigation, there will be investigations whose results and proposed corrective actions will be reviewed by the Ethics Review Panel (ERP). The corrective actions will be determined based on the facts and circumstances of the breach of conduct and the results of the investigation.

For more information on the process of investigation of alleged misconduct and violations of the Code of Conduct or this Policy, please refer to **QTerminals Whistleblower and Anti-fraud Procedures**.

9. REVIEW PROCESS

IT team will periodically evaluate the adequacy and effectiveness of this Policy. Depending upon the results of such reviews, amendments might be proposed and introduced.

Approved By:

Group CEO

Neville Bissett