IT POLICY

Q3 MANAGEMENT SOLUTIONS	**IT POLICY**	**Ref. No.: Q3-POL-IT**
		Revision: 00
		Effective Date: 31/12/2025

Revision no	Revision History	Date

APPROVAL AUTHORITY:

	Prepared By	Reviewed By	Approved By
Name	**Adi Danish bin Muhammad Amin**	**Shazlee Musa**	**Emiliawati Zainol**
Designation	**Data Analyst & IT Project Executive**	**Director**	**Managing Director**
Signature & Date	 31/12/2025	 31/12/2025	 31/12/2025

Q3 MANAGEMENT SOLUTIONS	**IT POLICY**	**Ref. No.: Q3-POL-IT**
		Revision: 00
		Effective Date: 31/12/2025

1.0 Introduction

Q3 Management Solutions Sdn. Bhd. (hereinafter referred to as "Q3Solutions" or "The Company") relies on information technology systems to deliver consulting, training, and advisory services efficiently and securely. As The Company manages business information, client data, intellectual property, and digital collaboration platforms, it is essential to establish clear governance over the use, protection, and management of IT resources.

2.0 Objectives

The purpose of this IT Policy is to establish clear guidelines and expectations for the use of IT resources within Q3Solutions. This policy aims to protect the organization's data, networks, and devices while ensuring that employees can work efficiently and securely.

3.0 Scope:

This policy applies to all employees, directors, interns, contractors, consultants, and third-party service providers who access or manage Q3Solutions' information technology resources.

It covers all IT assets and services owned, leased, managed, or used by The Company, including but not limited to:

- Company-issued devices
- Approved personal devices used for work purposes (where authorised)
- Cloud-based systems and applications
- Network infrastructure and internet access
- Digital communication platforms used for official business
- Company data in electronic form, whether accessed on-site, remotely, or via external networks

This policy applies regardless of work location, including office premises, home offices, client sites, and public environments.

4.0 Roles and Responsibilities:

4.1 Management is responsible for:

- Approving and endorsing this IT Policy
- Ensuring adequate resources are available to support IT governance and security controls
- Overseeing enforcement of the Policy

4.2 The designated IT personnel are responsible for:

- Implementing and maintaining IT security controls
- Managing user access provisioning and revocation
- Maintaining IT asset and software license records
- Coordinating backup and recovery processes
- Investigating and responding to reported security incidents
- Providing security awareness guidance as necessary

4.3 Department Heads / Supervisors are responsible for:

- Approving access requests for their respective team members
- Ensuring employees comply with this Policy
- Informing IT promptly of role changes, resignations, or access modification requirements

4.4 All Users (Employees, Interns, Contractors, Third Parties) are responsible for:

- Complying with this IT Policy
- Protecting The Company's IT resources and confidential information
- Safeguarding passwords and access credentials
- Reporting suspected security incidents promptly
- Using IT resources responsibly and ethically

5.0 Definition:

5.1 **IT Resources:** All hardware, software, cloud systems, network infrastructure, communication platforms, and digital tools owned, leased, or authorised by Q3Solutions for business use.

5.2 **Company Data**: Any information created, stored, processed, or transmitted through Q3Solutions' IT resources, including business records, client information, financial data, training materials, intellectual property, and internal communications.

5.3 **Confidential Information**: Information that is not publicly available and whose unauthorized disclosure may cause financial, reputational, or legal harm to Q3Solutions or its clients.

5.4 **User**: Any employee, intern, contractor, consultant, director, or third party authorised to access Q3Solutions' IT resources.

5.5 **Security Incident**: Any event that compromises or potentially compromises the confidentiality, integrity, or availability of Q3Solutions' IT resources or data.

5.6 **Multi-Factor Authentication (MFA)**: A security mechanism requiring two or more verification methods to access systems or applications.

5.7 **Acceptable Use Policy (AUP)**: The section of this policy outlining permitted and prohibited uses of Q3Solutions' IT resources.

6.0 Reference:

6.1 Personal Data Protection Act 2010 (PDPA)

6.2 Computer Crimes Act 1997

6.3 Communications and Multimedia Act 1998

6.4 Q3 Management Solutions Flexible Working Arrangement (FWA) Policy

6.5 Relevant Laws and Regulations: Including but not limited to data protection laws and cybersecurity regulations applicable to Q3Solutions' operations.

7.0 Relevant Records:

7.1 Inventory Records of IT Assets

7.2 Software License Management Records

8.0 Policy:

8.1 ACCEPTABLE USE POLICY (AUP)

8.1.1 Acceptable Use

- Employees are expected to use company-provided IT resources responsibly, primarily for business-related purposes that align with their job responsibilities.
- Acceptable uses include, but are not limited to, email communication, accessing Q3Solutions' databases, conducting research relevant to work tasks, and using approved software applications.
- Employees should exercise caution and discretion when accessing external websites, downloading files, or engaging in online activities to prevent security risks and potential harm to Q3Solutions' reputation.

8.1.2 Unacceptable Use

- Unauthorized use, access, or distribution of confidential, proprietary, or sensitive information is strictly prohibited.
- Employees must not engage in activities that violate local, state, federal, or international laws, including but not limited to copyright infringement, harassment, defamation, or illegal downloading of software or media.
- Any use of company-provided IT resources for personal gain, commercial purposes, or activities that could result in financial loss or damage to the organization's reputation is prohibited.
- Intentional or negligent actions that compromise the security, integrity, or availability of IT resources, including unauthorized access attempts, spreading malware, or tampering with network configurations, are strictly prohibited.

8.1.3 Monitoring and Enforcement

- Q3Solutions reserves the right to monitor, access, and review the use of company's IT resources to ensure compliance with this Policy, protect company's assets, safeguard confidential information, maintain system integrity, and comply with legal or regulatory obligations.

- Monitoring may include, but is not limited to, review of email communications, internet usage, system access logs, and file transfers conducted through The Company's systems.
- Such monitoring shall be conducted in a reasonable and proportionate manner, in compliance with applicable laws, including the Personal Data Protection Act 2010 (PDPA). Users should have no expectation of privacy when using company-owned or authorised IT resources for business purposes.
- Any violations of this Policy may result in disciplinary action, up to and including termination of employment, legal action, or other corrective measures deemed appropriate by Management.

8.2 SECURITY

8.2.1 Password Management

- All users are responsible for safeguarding their login credentials and ensuring that passwords are kept confidential.
- Passwords must:
  - Be at least 12 characters in length
  - Include a combination of uppercase letters, lowercase letters, numbers, and special characters
  - Not be easily guessable
  - Not be reused across multiple work-related platforms
- Passwords must not be shared with other individuals. Where shared access to systems is operationally required, access shall be managed through approved access control mechanisms or a company-approved password management solution.
- Passwords must be changed immediately if:
  - There is suspicion of compromise
  - An account has been accessed by an unauthorized party
  - An employee with shared system access leaves the organization
- MFA should be implemented for accessing sensitive systems or applications to enhance security.

8.2.2 Access Controls

- Access to The Company's IT resources shall be granted based on the principle of least privilege, ensuring that users are provided only the level of access necessary to perform their job responsibilities.
- **Access Provisioning (Joiner)**: New system access must be approved by the relevant Department Head or Director prior to account creation. Access rights shall be assigned based on the employee's role and responsibilities.
- **Access Modification (Mover)**: When an employee's role or responsibilities change, access rights must be reviewed and adjusted accordingly to ensure continued alignment with business requirements.
- **Access Revocation (Leaver)**: Upon resignation, termination, or completion of contract, all system access must be revoked promptly and no later than 24 hours from the employee's last working day. Shared passwords or system credentials previously accessible to the individual must be updated immediately.
- User access rights to critical systems shall be reviewed periodically to ensure appropriateness and remove unnecessary privileges.
- Administrative or elevated access rights shall be restricted to authorised personnel only and must not be granted unless operationally necessary.

8.2.3 Antivirus Software Usage

- Antivirus software must be installed, updated, and regularly scanned to detect and remove malware, viruses, and other malicious threats.
- Employees should report any suspicious activities or potential security incidents to the IT team promptly.

8.2.4 Network Security

- Network infrastructure must be configured with appropriate security controls, including firewalls, intrusion detection/prevention systems, and network segmentation, to prevent unauthorized access and protect against external threats.
- Wireless networks should be secured using encryption protocols and access controls to prevent unauthorized access and eavesdropping.

8.2.5 Security Awareness

- Ongoing Security Awareness Initiatives: While formal security awareness training is not currently conducted, employees are regularly engaged through various proactive awareness approaches to help them stay informed about potential security threats.
- Email Awareness: Employees are encouraged to share any suspicious or potentially harmful emails with the IT team, allowing the team to assess and raise awareness about common phishing and social engineering tactics.
- Screen Saver Reminders: Security awareness materials, such as tips on phishing prevention and password security, are periodically displayed on the Q3Solutions' screensaver as reminders to stay vigilant.

8.3 DATA CLASSIFICATION

8.3.1 Company data shall be classified according to its sensitivity and impact level to ensure appropriate protection and handling.

8.3.2 Public: Information approved for public release or already available publicly.

- Examples:
  - Marketing materials
  - Public event posters
  - Website content
- Handling:
  - No special access restrictions required
  - May be shared externally if authorised

8.3.3 Internal: Information intended for internal use within Q3Solutions that is not meant for public disclosure but would cause limited impact if exposed.

- Examples:
  - Internal SOPs
  - Non-sensitive operational documents
  - General staff communications
- Handling:
  - Accessible only to authorised employees
  - Must be stored in company-approved systems

8.3.4 Confidential: Information that is sensitive and may cause financial, legal, reputational, or contractual harm if disclosed without authorisation.

- Examples:
  - Client data and consulting materials
  - Payroll or HR data
  - Financial records
  - CRM exports
  - Strategic business plans
- Handling:
  - Access strictly limited to authorised personnel
  - Must be stored only in company-approved secure systems
  - Must not be transferred to personal accounts
  - Additional security controls

8.4 DATA BACKUP AND RECOVERY

8.4.1 Data Backup Procedures

- Q3Solutions shall ensure that critical business data stored in company-approved systems (including cloud storage and business applications) is protected through regular backup and retention controls.
- At minimum:
  - Critical operational data shall be backed up daily (automated where available).
  - Non-critical data shall follow a scheduled backup approach determined by the IT function based on business needs.
  - Backup retention periods shall be defined based on the importance, legal requirements, and operational needs of the data.
  - Backup access shall be restricted to authorised personnel to reduce the risk of unauthorised changes or ransomware impact.

8.4.2 Data Recovery Procedures

- In the event of accidental deletion, data corruption, device loss, or system failure, recovery actions shall be initiated promptly to restore business operations.
- Recovery procedures must include:

- Identification of affected systems/data and recovery priority
- Steps to restore data from available backup sources (including cloud restore/version history where applicable)
- Communication to Management for significant incidents impacting business operations or client data

8.4.3 Backup and recovery controls shall be periodically verified to ensure recoverability. At minimum, restore testing for selected critical data shall be conducted at least annually (or after major system changes) and documented for record purposes.

8.4.4 Employees must store work files only in company-approved cloud storage to ensure they are included in backup and recovery coverage.

8.5 IT ASSET MANAGEMENT

8.5.1 Asset Acquisition

- All IT asset acquisitions must be approved through the designated procurement process, following established budgetary and procurement policies and procedures.
- IT assets should be acquired based on business requirements and compatibility with existing infrastructure.

8.5.2 Asset Tracking and Inventory Management

- A comprehensive inventory of IT assets must be maintained, including detailed records of asset specifications, configurations, locations, and ownership information.
- Asset tracking tools or asset management software should be utilized to automate inventory management and facilitate accurate asset tracking and reporting.

8.5.3 Software License Management

- All software installations must be properly licensed and compliant with software vendor licensing agreements and usage rights.
- Software license management procedures should be established to track software licenses, monitor license usage, and ensure compliance with licensing terms and restrictions.

8.5.4 Asset Retirement and Disposal

- End-of-life IT assets should be retired and disposed of in accordance with environmental regulations and data security best practices.
- Disposal methods may include recycling, donation, or secure data destruction to prevent unauthorized access to confidential information stored on retired assets.

8.5.5 Asset Security

- Physical and logical security measures should be implemented to protect IT assets from theft, loss, or unauthorized access.
- Access controls, encryption, and asset tracking mechanisms should be employed to safeguard confidential information and prevent unauthorized use or tampering of IT assets.

8.6 WORK FROM HOME (WFH) RESPONSIBILITIES

8.6.1 Device Usage and Security

- All employees working from home are required to use company-provided devices for business activities, unless an alternative device is approved by the IT department.
- Implement basic security configurations, including password protection, firewalls, and screen auto-lock features.
- Be used exclusively by the assigned employee and devices must not be shared with family members or third parties.

8.6.2 Data and File Management

- All work-related documents, communications, and data must be stored and processed using company-approved systems and cloud storage platforms.
- Employees must not:
    - Store company or client data on personal cloud accounts
    - Save sensitive or confidential files permanently on local device storage unless operationally necessary
    - Transfer company data via unauthorised file-sharing platforms
- Temporary local storage (if required for operational reasons) must be transferred back to approved cloud storage as soon as reasonably practicable.

- Use of removable storage devices (e.g., USB drives) must be minimised and, where necessary, restricted to encrypted and company-approved devices only.
- When handling client or confidential data remotely, employees must ensure that:
    - Files are shared only with authorised recipients
    - Public or unsecured Wi-Fi networks are avoided when accessing sensitive systems, unless secured through approved security controls
    - Devices used for work are protected with password lock and encryption features where available
- Employees are responsible for ensuring that The Company data remains protected from unauthorised access by household members, visitors, or third parties.

8.6.3 Internet and Network Security

- Employees must not disable any firewalls, antivirus tools, or security applications while working remotely.

8.6.4 Communication and Availability

- Be available and responsive on official platforms including Microsoft Teams, Zoom, email, and WhatsApp during core working hours or as assigned.
- Attend virtual meetings promptly and in a presentable manner, with webcams turned on when required by the meeting organiser.

8.6.5 Data Confidentiality

- Lock screens when stepping away from workstations, even at home.
- Ensure that confidential or sensitive documents are not viewed, accessed, or printed in public or shared home areas.
- Prevent children, housemates, or any non-employee from accessing company-related materials.