

Purpose and scope

This policy provides a summary of the approved policies for the use of Information Technology (IT) at Mitie and applies to all employees, contractors, clients and suppliers regardless of location.

This policy must be read in conjunction with the following policies:

- Information Security Policy
- Acceptable Use Policy
- Identity and Access Management Policy
- Information Classification and Handling Policy
- IT Operations Policy
- Cloud Security

Policy objectives

Information is one of our most important assets – we depend on it to deliver services to our clients and its reliability and availability is crucial to our success. The objectives of this policy are to ensure that:

- The integrity and availability of our IT systems will be maintained;
- IT systems provide the right services to the right people at the right time;
- IT systems are protected from threats, are operated legally; and
- Information held on our IT systems is secured appropriately.

Requirements

Acceptable use: Our IT equipment should be properly cared for and used appropriately, in accordance with the **Acceptable usage policy**. Deliberate and serious misuse of our IT can have a damaging effect on our ability to deliver services to our clients – and could lead to disciplinary action.

Access: Access to our IT systems must be controlled. Systems are configured to meet security requirements and only the minimum access necessary will be allowed. Where access is allowed, it must be attributable and unique in line with the Identity and Access Management Policy

Monitoring: The use of IT systems is logged to facilitate fault resolution and the investigation of security incidents, and is monitored 24x7 to help identify system misuse.

Back-ups: Information which is critical to the continuity of business operations must be identified, with arrangements made for back-up in line with the IT Operations Policy and Information Classification and Handling Policy. This will mean that information can be promptly recovered if required, for example following a physical disaster or system failure.

IT disaster recovery: The appropriate preparation and arrangements must be in place so that IT can continue and recover following any failures or disasters **as agreed with the business on implementation** of the system.

Changes: Changes to IT systems (including hardware, software, peripheral devices, cables and so on) must only be conducted by Mitie IT or other Mitie employees under their supervision. Production system changes must follow documented **Change management policy**.

Incidents or Service requests: All requests for IT support or action must be submitted to the appropriate IT Service Desk and formally logged.

Information protection: All information must be stored in Mitie IT approved secure locations in line with the Acceptable Use Policy and Information Classification and Handling Policy. Data can only be stored outside of these locations with an approved Information Security Exception.

IT Operations: To support the integrity and availability of IT systems, they should be operated in a controlled manner in line with the IT Operations Policy, including:

- All critical activities associated with maintaining and supporting IT systems should be documented;
- IT systems should be proactively maintained and configured to reduce vulnerability;
- Appropriate means should be used to protect IT systems from threats, such as malicious code;
- IT systems should be supported by appropriately trained and available people who are provided with the correct tools to perform their duties;
- Only software that is fully licensed to Mitie and under the support of Mitie IT must be used on our IT equipment. It must not be copied for personal use; and
- The development of IT systems must be kept separate from production IT.

IT protection: Centralised IT systems that provide operational services must be housed in secure locations. The level of security should be based on the importance of the server - for example those running critical business applications would require greater security or those related to a client that requires a higher level of security. Security is the most critical element of all of IT Operations and no compromise will be permitted that impacts the overall security requirements.

Applications: Only approved applications supported by Mitie IT can be used for Mitie business. Any development of applications must be to formal procedures/standards, including security requirements as outlined in the Cloud Security Policy

Networks/Wireless: Our internal networks are only to be used by Mitie personnel and authorised contractors in relation to their Mitie duties. Access will only be provided via authorised devices. Guest wireless networks are provided at some office locations for use by third parties and authorised Mitie users.

IT purchasing: All IT and IT related services must be procured through Mitie IT approved suppliers.

Disposal: All IT equipment must be returned to the IT team in order that it can be disposed of in a controlled manner to protect any information stored on the equipment.

Responsibilities

All staff, contractors, clients, and 3rd parties have a responsibility to maintain the confidentiality, availability, and integrity of the information and assets they have access to as outlines in the Information Security Policy.

The Chief Executive Officer (CEO) is responsible for:

- Reviewing, endorsing and achieving this policy's aims.

The Chief Technology & Information Officer (CTIO) is responsible for:

- Administering this policy on behalf of the CEO; and
- Developing and rolling out the supporting strategies.

The Chief Information Security Officer (CISO) is responsible for:

- Administering the Cyber, Data and Information Security policies on behalf of the CEO & CTIO
- Developing and rolling out supporting Information Security policies

IT Managers / Suppliers are responsible for:

- Ensuring that this policy and supporting procedures are distributed, implemented and complied with; and
- Providing IT that supports the policy requirements.

Managers are responsible for:

- Implementing and enforcing the processes and procedures;
- Ensuring that their people are aware of their responsibilities and receive appropriate training
- Addressing any inappropriate behaviour; and
- Ensuring the leaver process is followed within IT for system accounts and hardware returns

Employees are responsible for:

- Carrying out their work in line with this policy and associated procedures;
- Challenging any behaviour that falls short of the expectations of this policy; and
- Identifying any breaches of this policy and reporting them to their line manager.

What will successful implementation of this policy achieve?

- Reliable IT systems with high levels of availability;
- Secure information, with low number of incidents; and
- Adherence to supporting policies, procedures and standards



Phil Bentley
Chief Executive Officer
Mitie Group PLC

1st March 2024