Purpose

Security incidents can expose personal and sensitive data to those who should not have access to this data, potentially causing reputational damage and the risk of incurring substantial fines. This policy covers the appropriate response of all employees of AMD when an incident occurs.

Scope

This policy applies to all employees and contractors of AMD with access to the IT Facilities or network.

Definition

A security incident is defined as an incident where any service or information stored or processes by AMD has been lost, destroyed, altered, copied, transmitted, stolen, used or accessed unlawfully by unauthorised individuals accidentally or on purpose.

This includes but not limited to:

- The loss or theft of any device, personal or owned by AMD, that stores data or email account.
- The loss or theft of any device, personal or owned by AMD, with a VPN client to connect to AMDs VPN.
- An attempt by unauthorised persons to gain access to data or computer systems of AMD.
- The presence of ransomware or computer virus on any device that has access to the AMD network.
- Any AMD user account compromised by phishing scam.
- Emails containing personal data sent in error to the incorrect recipient.

Reporting

All incidents or suspected incidents must be reported to support@aptustechnology.co.uk, sonia.bateman@amdenvironmental.co.uk as soon as a risk or breach is identified. Where a loss of personal or sensitive data may have occurred, this must also be reported no later than 24 hours but ideally as soon as the loss is noticed.

Where a loss or theft is reported to a regulatory body such as the police, a copy of the report must be submitted to sonia.bateman@amdenvironmental.co.uk

The report should include full and accurate details of the incident containing the following:

- The nature of the incident (theft or loss of equipment, hacking or phishing attack etc).
- What type of data that was involved in the loss.
- Details or any 3rd parties involved in the loss.

The IT Support company, which is Aptus Technology Ltd, will record and log the incident as well as Sonia Bateman.

Investigation

The Incident Response Team is formed of the IT Support company which is Aptus Technology Ltd with Sonia Bateman acting as the incident manager.

The Incident Manager will perform an initial investigation into the incident as soon as practically possible upon receipt of the incident being reported.

The Incident Manager will establish the following:

- The nature of the incident.
- Classify the incident for workflow response.
- If personal or sensitive data has been exposed, AMD should identify the associated individual/s.
- Assess any risks to the AMD data, the company network, servers and to the company overall, with the impact of the risks.
- Any legal consequences.

Where a breach of personal or sensitive data has occurred, then a Managing Director must be informed.

Response

The Incident Response Team will determine the appropriate course of action and resources required to limit the impact of any data breach. This may mean isolating devices and servers from the network or making entire networks or services unavailable.

The Incident Manager will record all actions taken and decisions made in the incident log.

Where criminal activity may have taken place then all efforts will be made to preserve evidence, this may take precedence over system recovery.

Appropriate steps will be taken to recover the data or restore services to resume to “business as normal” state.

Named individuals exposed in any data breach must be contacted with details of the incident and any risks to them.

AMD staff should not pressurise the incident response team or IT Support company to restore services at the expense of due diligence in carrying out their duties.

Review

The IT Support company will review each incident to identify new risks, new response workflows and changes to procedures or policies, that are required to prevent similar incidents and to highlight any non-conformance with the policy, which may result in disciplinary proceedings.

The review will be forwarded to the incident response team for evaluation and to approve the proposal if a policy change is recommended.

Regardless of the foregoing, this policy will be reviewed no less frequently than every 12 months.

Responsibilities

The End User is responsible for reporting all incidents to the incident response team and IT Support company.

The IT Support company is responsible for recording all security incidents, limiting spread of the incidents, and containing data loss, which includes implementing technical controls to prevent security incidents. The incident response team is responsible for reviewing incidents and recommending changes that have been highlighted by the IT Support company We now have Microsoft Security which puts an suspected phising emails into quarantine to be reviewed by admin before releasing.

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to [*OFFICE MANAGER/ IT Department*].
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media policy.

Our [*Security Specialists/ Network Administrators*] should:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our [*Security Specialists/ IT Administrators.*]

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action.

SIGNED:

Mr Jon King
Managing Director
01.12.2023

Mr Marcus Sullivan
Managing Director
01.12.2023