Infrastructure Security Policy

Policy - Infrastructure Security

Version No	Revision Date	Description of Change	Author	Approved by	Approval Date
1	28/04/2023	Create initial policy	Shane Bauskis	Peter Suchting	28/04/2023
2	25/05/2023	Minor wording correction and additions	Steven Ford	Peter Suchting	31/05/2023

3.9.1 Purpose

Attekus wish to provide a secure infrastructure in order to protect the integrity of data and mitigate risk of a security incident. This policy may refer back to other company policy documents.

The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure infrastructure. The Infrastructure Security Policy will provide the practical mechanisms to support the company's comprehensive set of security policies. However, this policy purposely avoids being overly specific in order to provide some latitude in implementation and management strategies.

3.9.2 Scope

This policy covers all IT systems and devices that comprise the corporate network or that are otherwise controlled by the company.

3.9.3 Policy

3.9.3.1 Clear Desk and Clear Screen Policy

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day when on site and when they are expected to be gone for an extended period.
- Computers must be locked when workspace is unoccupied.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Confidential information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock mobile devices when not in use.

3.9.3.2 Event Logging

The logging of events is an important component of the company’s management practices. Logging will vary depending on the system being monitored and the type of data the system holds. The following sections detail the company's requirements for logging and log review:

Internal Systems

Logs are monitored through various Microsoft services, including but not limited to: Azure Dashboards, Microsoft Defender For Cloud and Microsoft 365 Defender. Azure is used, where applicable to monitor capacity and events. Alerts are received for all critical events.

The following must be enabled, where available:

- Critical events;
- Audit tracking logs and change tracking;
- Service logs;
- Login attempts;
- Capacity management.

Alerts are also received for the following:

- Application alerts;
- Vendor updates.

Logs are reviewed every 3 months by the Head of Technology. Where issues have occurred further investigation will be conducted as per the Security Incident and Data Breach Response Procedure.

Staff devices are home based and are required to access private cloud based infrastructure either securely over an encrypted Azure VPN connection or via Microsoft/Azure portals via Azure AD.

Log Management

Logs are protected against tampering and unauthorised access. All logs are encrypted - stored securely in Azure with secure access policies in place.

Logs are retained for a minimum of 90 days.

Network Compartmentalisation

Segmentation of higher risk networks from the company's internal network is required and must be enforced with policy level access controls.

An encrypted Azure VPN connection is required for staff to access infrastructure/resources hosted on the Attekus Azure VNET e.g. Bookable databases.

Firewalls

- Firewalls must provide secure access (through the use of encryption) with management access limited to requirement. Administrative access must be limited to only networks/devices where management connections would be expected to originate.
- The firewall resource itself is protect/managed by Azure PaaS but administrators are required to apply appropriate rules and access controls.
- No unnecessary services or applications are to be enabled on firewalls. The company uses `hardened' systems for firewall platforms, or appliances.
- Clocks on firewalls and other cloud infrastructure is managed by Azure PaaS. Among other benefits, this aids in problem resolution and security incident investigation.
- The firewall policies must be documented and audited quarterly. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved. Policies must be monitored for use.

Networking Hardware

- All networking hardware is managed by Azure PaaS (Platform as a Service).

Virtual Private Servers

The following statements apply to the company's use of such servers:

- Unnecessary files, services, and ports should be removed or blocked. The Server should be hardened to the operating system manufacturers best practice guidelines.
- All Servers must be protected by a firewall from User and Public Networks with Antivirus and Intrusion Prevention enabled.
- Unused services and ports must be disabled

Note: Attekus currently has one Virtual Private Server / Virtual Machine which is used only for internal testing purposes and restricts access through a Secure VPN connection.

3.9.3.3 Security Testing

Scans are performed to detect the following in the entire infrastructure:

- **Vulnerability assessments** are carried out in real time through the use of Microsoft 365 Defender and Microsoft Defender for Cloud (which includes routine Database Checks). In addition to this, Intruder IO carries out routine scans on Bookable.
    - Alerts are received by the Head of Technology, Director of Customer Success and the Director of Product;

Security audits are carried out quarterly by the Head of Technology;

Penetration testing is carried out every year on the Bookable system by a third-party security specialist prior to the Attekus Certification audit. Intruder io is used to monitor events daily.

3.9.3.4 Disposal of Information Technology Assets

IT assets often contain sensitive data. When such assets are decommissioned, the following guidelines must be followed:

- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults
- Physical destruction of the device's data storage mechanism (such as its hard drive or solid-state memory) is required. If physical destruction is not possible, the Head of Technology must be notified.

3.9.3.5 Network Compartmentalisation

The infrastructure is compartmentalised to limit the access to any deliberate intruder to the least possible data.

Externally accessible systems are also protected by policy level access controls with anti-virus and intrusion prevention services enabled.

3.9.3.6 Network Documentation

At a minimum, network documentation must include:

- System configurations
- Firewall policy
- Access Control Lists

Access Control Lists are reviewed at least annually by the Head of Technology or any time changes occur e.g. critical events or changes to the environment.

3.9.3.7 Antivirus / Anti-Malware

The company provides the following guidelines on the use of antivirus/anti-malware software:

- All company systems (workstations, laptops) must have antivirus/anti-malware software installed.
- Company systems must maintain a current "subscription" to receive patches and virus signature/definition file updates.
- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.

For cloud based infrastructure (e.g. servers and databases) Attekus depend on Azure PaaS to intrinsically manage all antivirus, anti-malware, patches and updates.

3.9.3.8 Acceptable Use Policy

The company provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for the company's software must be stored in a secure location.
- Software should be kept reasonably up to date by installing new patches and releases from the manufacturer.
- Vulnerability alerts should be monitored for all software products that the company uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

The Acceptable Use Policy contains more information and should be referred to for full details.

3.9.3.9 Change Management

Any changes done to the network must be done in guidance with the company’s project control framework / procedures or as per Section 4.1 of the QISMS.

3.9.3.10 Suspected Security Incidents

When a security incident is suspected that may impact a device, Staff should refer to the company's Data Breach and Incident Response Plan for guidance.

3.9.3.11 Redundancy

Redundancy is built into the cloud-based applications and Azure platform and other cloud-based servers with virtual servers in multiple locations.