Annington Information Security Policy

Access to this document is restricted to IT staff. Elements appropriate to other people are included in the Employee Handbook.

1. Management responsibilities

This document supplements policies contained in the Employee Handbook and is a formal statement of policies and procedures that have been in place since 1997.

The document is the responsibility of the IT Director.

The IT Director is responsible and accountable for:

all IT security tasks

cyber security

all compliance requirements

updating and implementing this policy

The Information Security Policy is kept under constant informal review. In particular, it is reassessed when new threats become apparent.

It was last formally reviewed in February 2021.

2. Risks

Annington holds no personal financial data such as credit card details, although bank account details are held for suppliers, some of whom are sole traders.

Sensitive employee data is held securely in Cascade HR’s cloud system. Access is via Azure, using Annington network credentials with two factor authentication. Other employee data is held in secure folders on the Annington network with restricted access.

Address details for the MQE could be considered as sensitive. Although partly in the public domain, they would be of great interest to state sponsored entities and terrorist organisations.

Customer information is shared only with agents who need it to fulfil the role required of them by Annington (for example solicitors and sales agents). Sales agents manage the relationship with prospects, so no such data is held by Annington other than via general email correspondence.

Sales information is considered to be of little interest to identity thieves as it is already primarily in the public domain (via telephone directories, electoral registers, etc.) Accidental or wilful destruction of data by staff or hackers is a significant risk.

Theft or accidental distribution of data is made less likely by restrictions on the use of portable media (e.g. USB data sticks). Regular backups make recovery of data straightforward in normal circumstances.

3. Organisation and Personnel

ITC provides ‘Information Security Officer As A Service’ to Annington, working closely with the IT Director and Vale Systems.

Employees

References are always obtained for new staff before they join the company. After joining, they receive the Employee Handbook. It contains key security guidelines and details the consequences of breaking security regulations. New staff are also briefed on security policy as part of the induction process.

E-mail is used to keep staff up-to-date with information on new security threats, for example viruses or social engineering.

All new staff sign to confirm their understanding and agreement to their principal statement of employment, the employee handbook and associated policies.

Leavers

Security badges are deactivated, restricting physical access to the office.

Logon accounts are deleted or disabled. If they are disabled, remote access privileges are withdrawn, an expiry date is set on the account and the password is changed.

Leavers are encouraged to remove all personal data from their mailboxes and personal folders before they leave.

Personal folders and e-mail accounts of leavers are assigned to a manager who is allowed six months to identify any document that might be worth retaining before the folders and accounts are deleted.

Third parties

There are written agreements with all other parties who have access to the office (security guards, cleaners, etc.)

People who access the server and communications room are accompanied by a member of the IT team.

4. Information Classification

Information classification is not applied universally, but restrictions are applied as appropriate with employee and MQE address information considered most sensitive.

Each member of staff has a "personal" folder which is confidential.

Other data is considered to be "open" but restrictions are applied to functionality (for example authorisation of invoices or a Site Instruction Form). The Annington Information Management System limits visibility and editing to those who need it.

A combination of Active Directory authentication and built-in software restrictions is used to enforce the above.

5. Vulnerability Management

Nessus is used to scan all devices (from telephone handsets to firewalls) on the network daily. Risks are classified as high, medium or low with critical risks receiving top priority in terms of overall task scheduling.

WSUS and Heimdal are also used to identify unpatched systems and to apply updates.

Annington subscribes to an Endpoint Detection and Response (EDR) service with a Security Operations Centre (SOC) that assesses and reports on identified threats.

6. Software

No software may be brought into the organisation without the approval of IT. Staff are reminded of this when they log on.

Security requirements are always considered during systems development. While access to information is generally "open", access to specific functions may be restricted and audit logs are kept.

Security is a major consideration when buying systems from third parties. No software is considered unless it meets Annington's requirements.

Changes to systems are tested before going live. Test databases are used for major changes and any change that might affect live data.

Annington has implemented Windows Server Update Services and Heimdal to control distribution and application of (mainly) security-related patches.

Major Operating System changes are only made after thorough evaluation and testing by Vale Systems, Annington's IT support company.

Annington uses Microsoft Defender (ATP) to monitor and control anti-virus software and settings on all PC's connected to the Annington network.

WatchGuard's Advanced Persistent Threat protection has been enabled on the firewall.

All in-house applications and 3rd party software are backed up and kept in a secure location off-site.

7. Hardware

Equipment may not be used on the Annington network without approval from IT.

Redundant computer equipment is disposed of by the IT team using WEEE approved contractors. When equipment is donated to a charity, its data is wiped beforehand.

The Employee Handbook contains guidelines for the use of equipment supplied by Annington.

Security is always considered before acquiring new hardware and before connecting it to Annington's network.

Every PC is allocated to an individual who bears responsibility for ensuring that policy is applied.

Software installation conforms to a “gold build” that is applied via Active Directory and Heimdal.

8. Documentation

Policy is documented here and in the Employee Handbook (given to all employees on joining and available online via the personnel system).

Systems and processes are documented to a level that is appropriate for a company of Annington's size. User manuals are generally incorporated in business process descriptions (in preference to separate publication).

AIMS has a built in help system where users can record their own tips and guidance.

AIMS contains descriptions of complex and unusual routines to help with general maintenance and development and there is a separate document detailing the software design, development and deployment process.

Hardware and communications networks are documented in the Business Continuity Plan.

9. Computer Media

Annington uses an offsite backup service but also maintains local backups on magnetic media. These are both physically and electronically labelled. They are kept in a secure location onsite.

Backups are not transported without prior approval from the IT Director.

A number of PC's have USB, CD or DVD write capability. These are disabled for all but a selection of IT personnel and senior, trustworthy employees.

No single person has control over all copies of backed up data.

BitLocker is used to encrypt laptops.

10. Identification and Authorisation

All users of Annington computers are required to enter a user id and pass phrase.

Logons are logged.

Azure reports anomalous logons (for example when a user logs in from a new location).

Attempts to access restricted folders or data are logged.

Pass phrases expire automatically after 60 days and have a minimum age of 1 day.

"Complex" pass phrases are enforced.

Pass phrases may not be re-used within 10 password changes.

Accounts are locked after 5 consecutive failed attempts to enter a password within 24 hours. The IT Help Desk is notified automatically and immediately if an account is locked.

The pin length on mobile devices is 8.

Minimum password length is 13 characters.

Account lockout duration is 0 minutes, meaning that the account will be locked out until an administrator explicitly unlocks it.

11. Administrative Accounts

Policy is not to have accounts with the name “Administrator”, so the "Administrator" account has been disabled and removed from all possible Active Directory groups.

In rare cases where administrator privileges are required, even temporarily, they must be approved by the IT Director.

Users may not change their own account privileges.

Users do not have administrative rights on their laptops. Activities that require administrative rights are managed via Heimdal and Local Administrator Password Service is used to handle situations where users lose local passwords.

12. Remote Access

Access to the network is restricted to devices issued, configured and controlled by Annington. Exceptions are made for trusted third parties such as Eversheds and EDC Lord.

Citrix is used to allow remote working and remote desktop connections.

Two Factor Authentication is enforced for Citrix and Azure AD related services (e.g. Cascade).

Members of the IT team may use a VPN to connect to a desktop PC; this is enabled and controlled via the Watchguard Mobile VPN with SSL client. This option may also be used to allow change of network passwords.

A penetration test is to be carried out annually.

13. Web Sites

All traffic on the Annington web sites is encrypted.

The web sites are not transactional and are not connected to the Annington network, so the risk posed by infiltration is very low.

The Privacy Policy is reviewed regularly to maintain compliance with the Data Protection legislation.

Webbed Feet maintains the sites and applies security patches to the hosts as they become available.

14. System Security and Logging

All PC's are configured to synchronise to a single time (to help logging and tracking of changes).

SQL triggers are used to log all changes to selected tables.

Microsoft's standard logging is in use.

The server log files are accessible only by system administrators.

Watchguard's Data Loss Prevention service is used to help detect outgoing transmission of personal data.

All events are logged but this makes it difficult to identify real threats. Implementation of Managed Detection and Response during 2021 will pass the responsibility to ITC’s Security Operations Centre.

15. Change Management

Network changes are agreed in writing between Vale and the IT Director.

Users are consulted beforehand if a change will affect availability of systems.

Change activity is recorded in detail by Vale and communicated via e-mail with the IT Director.

16. Communication

Ports are closed to SMTP. All ports are blocked unless explicitly allowed.

Network administrator privileges are restricted to Vale employees who need them and to the IT Director. To facilitate logging and management, these privileges are available only via administrative accounts that are separate from normal user accounts.

All network hardware is password protected and is installed in the server and communications room where applicable.

An Intrusion Detection System is operational on the firewalls used for internet access.

Firewalls restrict unauthorised external access.

Wireless networks are password-protected.

A guest wireless network provides internet access for guests without allowing access to the main Annington network.

Safeguards have been considered for all forms of communication in use, as outlined below:

E-mail

Outlook Web Access is encrypted.

Encryption of standard e-mail is reviewed with each upgrade of the mail server.

E-mail traffic is scanned for viruses, spam and bad links by Symantec Cloud and a WatchGuard firewall before it hits the Annington network and is presented to the Exchange server (which also has its own spam filtering). Heimdal checks for viruses, spam and bad links.

Annington's e-mail can only be downloaded onto mobile devices that are encrypted.

DNS Services

Are only used within the Annington domain. No special safeguard is considered necessary.

Web Sessions

The WatchGuard Firewall is used to control and monitor web access.

Java/JavaScript/ActiveX

Annington uses standard Microsoft settings to control use of Java/Javascript and ActiveX.

Heimdal is used to remove older versions.

Cookies

Threats from cookies are reduced through means described in other sections of this policy, primarily the firewall.

Virtual Private Networks

VPN's are covered above.

17. Backup

All data is backed up at regular intervals during the day to a secure server in a remote location.

Additionally, local backups are made and kept in a secure area with month end backups being kept for at least seven years.

All backups are encrypted (the password is stored in a software-based password safe).

18. Physical Protection

The building is protected during working hours by security staff. Outside working hours, the main door is locked and a security card must be used to gain entry.

The main office door is locked in the evenings and at weekends. A security card must be used to gain entry.

The main door is also protected by a burglar alarm linked to a 24/7 security monitoring service.

The server and communications room has a keyguard system. The default code is changed on a regular basis (every 6 months) and is known only by the IT team. It is changed if a member of the IT team leaves the company.

19. Incident/Contingency Planning

The Help Desk is the first contact point for all systems issues at Annington; it escalates any potential breach immediately and directly to the IT Director.

Depending on the nature and scale of the incident, either the IT Security Incident Handling Process or the Business Continuity Plan (or both) would be invoked. The decision would be made by the IT Director in conjunction with the CEO or CFO.

20. Cyber Security Skills

The IT team maintains a high level of awareness of cyber security threats through its relationship with ITC and its subscriptions to cyber security news channels. Gaps in its knowledge are addresses via training (webinars, white papers, etc.).

An online cyber security training course must be completed and passed by all staff. Refreshers are issued every sixty days and must also be passed.

Annington is working towards Cyber Essentials Plus, a qualification recognised by the National Cyber Security Council.