IT Security Addendum

Version 2.0 - January 2025

Classification: INTERNAL

1. Purpose and Scope

This IT Security Addendum provides supplementary security guidance issued by the Chief Information Security Officer. Where this addendum conflicts with existing policy documents, the addendum takes precedence as the most recently published guidance.

This addendum applies to all employees, contractors, temporary staff, and third-party users of company IT systems. Compliance is mandatory and will be audited quarterly by the IT Security team.

This addendum was developed following the annual security risk assessment (December 2024) and reflects updated threat landscape analysis, penetration testing findings, and regulatory changes.

2. Enhanced Password Requirements

Following a recent security audit, the following enhanced password requirements supersede Section 4 of the Internal Policy Handbook. All passwords must now be a minimum of 12 characters in length (increased from 8 characters).

Password rotation period is reduced to 30 days for all users (previously 90 days). Privileged accounts must rotate passwords every 14 days. Automated rotation is enforced through the Identity Management platform.

Passphrases are now accepted and encouraged as an alternative to traditional passwords. A passphrase must contain at least 4 words and a minimum of 20 characters. The first character of each word must be capitalised.

Failed login threshold is reduced to 3 attempts (from 5), after which the account is locked for 60 minutes. IT Security may override this lockout for critical operational accounts on a case-by-case basis.

3. Network Access and Remote Connectivity

Access to company systems from public Wi-Fi networks is now strictly prohibited, including when using VPN. Employees must use either the corporate network, a company-provided mobile hotspot, or a personal mobile data connection.

All remote access sessions are limited to a maximum of 8 hours and require re-authentication. Session recording is enabled for all privileged remote access sessions.

Split-tunnel VPN configurations are no longer permitted. All network traffic from company devices must route through the corporate VPN, regardless of destination.

Network access from personal devices is restricted to the Guest network segment, which provides internet-only access with no connectivity to internal systems. Access to internal systems from personal devices requires BYOD enrolment (Section 13 of the handbook).

Geographic access restrictions are now enforced: access from outside the UK, EU, and US requires pre-authorisation from IT Security, submitted at least 72 hours in advance.

4. USB and Removable Media

Effective immediately, USB storage devices are prohibited on all company endpoints. This supersedes the previous policy permitting encrypted USB devices with IT Security approval.

This prohibition includes USB flash drives, external hard drives, SD cards, and any other removable storage media. USB ports on company devices are disabled via endpoint protection policy.

Exceptions may be granted only by the CISO for documented operational requirements. Exception requests must include business justification, risk assessment, and proposed compensating controls. Approved exceptions are valid for a maximum of 30 days.

Data transfer between systems must use approved secure channels: SFTP, encrypted email, or approved cloud storage services. Physical media transfer of any kind requires CISO approval.

USB peripherals (keyboards, mice, headsets) remain permitted but must be non-storage devices. IT Security maintains an approved peripherals list.

5. Visitor Access to Secure Areas

Visitors may be granted temporary escorted access to secure areas, including server rooms, under the following conditions: the visit is pre-approved by the IT Operations Manager, a documented business justification is provided, and the visitor is escorted by an authorised employee at all times.

This supersedes the blanket prohibition on visitor access to Restricted Zones. The updated policy recognises that certain maintenance activities (HVAC servicing, electrical inspections, fire safety assessments) require third-party access.

Visitor access to server rooms is limited to a maximum of 4 hours per visit. All visitor activities in Restricted Zones must be logged in real-time by the escort using the Visitor Activity Log (FA-008).

Visitors must not bring electronic devices (phones, laptops, cameras) into Restricted Zones without prior written approval from the CISO. All approved devices must be inspected and logged before entry.

Unescorted visitor access is never permitted under any circumstances, regardless of the visitor's role or purpose. Escorts must remain within visual line of sight of the visitor at all times.

6. Training Frequency

Security awareness training must be completed quarterly by all employees, superseding the annual requirement in the handbook. Quarterly training modules will be shorter (30 minutes each) but more frequent to improve retention.

Each quarterly module will focus on a specific topic: Q1 -- Phishing and Social Engineering, Q2 -- Data Handling and Classification, Q3 -- Incident Response and Reporting, Q4 -- Physical Security and Clean Desk.

Phishing simulation frequency is increased to weekly. Results are tracked per-department and published on the security dashboard. Departments consistently scoring below 90% pass rate receive targeted intervention.

Employees who fail any phishing simulation must complete an additional 15-minute micro-learning module within 48 hours. Failure to complete remedial training within the deadline results in temporary email quarantine.

New starters must complete the onboarding security module within 7 days (reduced from 30 days). The module includes a practical assessment that must be passed with a score of 80% or higher.

7. Data Sharing Approval Process

For operational efficiency, sharing of INTERNAL-classified data with approved external partners does not require manager approval, superseding the general requirement in Section 3 of the handbook.

A list of approved external partners is maintained by the Procurement team and published on the company intranet. Partners on this list have signed appropriate NDAs and DPAs.

Sharing of CONFIDENTIAL data externally always requires dual approval: the data owner and the CISO. Automated workflows in the DLP (Data Loss Prevention) system facilitate rapid approvals with target response time of 4 hours.

All external data sharing, regardless of classification, must be logged in the Data Sharing Register maintained by the Data Governance team. The register records: date, data description, classification, recipient, method of transfer, and approver.

RESTRICTED data may never be shared externally without board-level approval. Digital sharing of RESTRICTED data requires the use of the company's secure data room solution with full audit logging.

8. Encryption Standards Update

Encryption of sensitive data at rest is mandatory for all CONFIDENTIAL and RESTRICTED data, using AES-256 or equivalent approved algorithms. This supersedes the more general encryption requirements in the handbook.

Data in transit must be protected using TLS 1.3 or higher. TLS 1.2 is permitted only for legacy systems with a documented exception, which must be remediated within 6 months.

Full-disk encryption is mandatory on all company endpoints (laptops, desktops, mobile devices). BitLocker (Windows) and FileVault (macOS) are the approved solutions. Recovery keys must be escrowed to the central key management system.

Email encryption is required for all emails containing CONFIDENTIAL or RESTRICTED data. The approved solution (Microsoft 365 OME) provides automatic encryption based on sensitivity labels.

Encryption key management must follow the Key Management Standard (ITS-009). Keys must be rotated annually, and key custodians must be registered with IT Security.

9. Staff Attendance and Office Presence

All employees are expected to maintain a minimum of 5 days per week in-office presence, effective from 1 February 2025. This supersedes the remote work provisions in Section 2 of the handbook.

Exceptions to the in-office requirement will be considered on a case-by-case basis by the HR Director in consultation with the employee's line manager. Medical exemptions require occupational health documentation.

Hot-desking is the default arrangement for all employees. Personal desk assignment is available only for employees with documented ergonomic or medical requirements.

Core presence hours are 09:30-15:30. Arrival and departure flexibility is permitted outside these hours provided the standard 37.5-hour week is worked. Time tracking is managed through the corporate HRIS.

Employees with existing remote work agreements (pre-dating this addendum) will transition to the new attendance requirement over a 3-month grace period, ending 30 April 2025.

10. Endpoint Detection and Response

All company endpoints must have the approved EDR (Endpoint Detection and Response) agent installed and running. Currently, the approved solution is CrowdStrike Falcon.

Employees must not disable, uninstall, or interfere with the EDR agent. Tampering with endpoint security software is treated as a serious policy violation.

The EDR system monitors for suspicious activities including: unusual process execution, lateral movement, privilege escalation, unauthorised network connections, and data exfiltration attempts.

Alerts from the EDR system are triaged by the SOC. High-severity alerts trigger automatic device isolation pending investigation. Affected employees will be contacted by the SOC for interview.

Monthly endpoint compliance reports are generated and shared with department heads. Departments with less than 95% compliance on EDR deployment receive a formal non-compliance notice.

11. Secure Software Development

All development teams must integrate security testing into their CI/CD pipelines. Static Application Security Testing (SAST) must be run on every Pull Request. Builds with Critical or High severity findings must not be merged.

Dynamic Application Security Testing (DAST) must be run at least weekly against staging environments. Findings are tracked in the vulnerability management platform and must be remediated within SLA.

Dependency scanning must be enabled in all repositories. Libraries with known Critical vulnerabilities must be updated within 48 hours, High within 5 working days.

Secrets management: hard-coding of credentials, API keys, or certificates in source code is prohibited. All secrets must be managed through the approved vault solution.

Security architecture review is required for all new services and significant changes to existing services. Review requests must be submitted at least 10 working days before the planned deployment.

12. Vulnerability Management

Critical vulnerabilities must be patched within 24 hours of publication. High-severity vulnerabilities must be patched within 7 days. Medium and Low vulnerabilities must be patched within 30 days.

Patching schedules are maintained by IT Operations. Emergency patches outside the normal maintenance window require Emergency Change authorisation.

Vulnerability scanning of all internet-facing systems occurs daily. Internal network scanning occurs weekly. Results feed into the vulnerability management dashboard.

Systems that cannot be patched within SLA must have a documented risk acceptance, signed by the system owner and the CISO. Compensating controls must be implemented as specified by IT Security.

External penetration testing is conducted annually by an approved third-party provider. Internal red team exercises are conducted quarterly. Findings from both are tracked to remediation.