AIT TECHNOLOGY | BUSINESS IMPLEMENTATION SERIES

Cybersecurity operations manual for businesses

A practical operating framework with department responsibilities, sector adaptations, everyday controls and incident playbooks. Customise it to the way your organisation actually works.



AI-generated editorial illustration; fictional people and systems.

Tailored to your business

AIT Technology can customise these procedures and build bespoke software, AI workflows and integrations. Scope, testing, pricing and support are agreed before implementation.

Version 1.0 | 18 November 2026 | UK business context

Starting framework: approve company-specific scope and owners before adoption. No certification, guaranteed compliance or emergency response service is implied.

How to use this manual

Owners, managers, department leads and the people responsible for IT. UK business context; specialist and regulated environments need additional assessment.

Read the operating framework, assign department owners, select relevant sector scenarios, and adapt each procedure. The companion interactive PDF contains one reusable record per procedure. Save a separate copy for each case. Do not put passwords, API keys or recovery codes in these records.

Contents

Process at a glance

Operating framework

Department responsibilities

Business and sector scenarios

Step-by-step procedures

Records, approvals and maintenance

Custom implementation and sources

Process at a glance

01. Prepare and assign owners	02. Identify and report	03. Contain safely	04. Assess and recover	05. Learn and improve

Use a named owner and recorded result at every handoff. Pause affected actions when safety, access or approval conditions are not met.

Operating framework

1. Approve a company-specific version

This is a comprehensive starting framework, not a completed policy for an unidentified business. The owner must approve a named version covering the actual legal entities, sites, systems, suppliers, working hours and services. Identify exclusions and existing contractual obligations. Give each control a responsible person, deputy, review date and evidence location.

AIT Technology can tailor this manual to your company, departments and operating scenarios, and help implement bespoke workflows, integrations and software. Begin with discovery and agree the scope, responsibilities, acceptance tests and support arrangements. This publication does not promise certification, legal compliance, specialist forensic services or round-the-clock incident response.

2. Name decision-makers before an incident

The business owner is accountable for risk and approves exceptional expenditure and service restoration. The incident lead coordinates decisions and the incident log. IT carries out authorised technical containment and recovery. Department leads manage safe workarounds. The privacy lead assesses personal-data implications. Finance contacts the bank for suspected payment fraud. One communications owner approves customer and supplier updates.

Small companies may combine these roles, but must still name deputies and separate approval from execution where practical. Keep an offline contact sheet with trusted provider and bank contact routes. Never put passwords, recovery codes or API keys in the manual. Agree who can temporarily disable an account or suspend a service, including out of hours.

3. Map what must keep working

List email, identity, finance, files, website, customer records, operational equipment and supplier services. For each, record business owner, technical contact, critical data, integrations, recovery dependencies and maximum tolerable interruption. Agree recovery-time and acceptable-data-loss objectives with the business; a backup schedule alone does not establish either.

Classify information as public, internal, confidential or restricted using your own definitions. Record where sensitive information is stored and who needs access. Keep access and retention decisions consistent across file shares, email, backups and SaaS services. Prioritise a few critical workflows instead of treating every laptop and document as equally urgent.

4. Establish the everyday security baseline

Maintain named user accounts, least privilege, stronger sign-in protection where supported, approved password storage, managed devices, supported software and a documented update process. Separate everyday and administrator access. Review changes when people join, move roles or leave. Secure recovery methods and test an emergency access route without sharing credentials.

Keep backups protected from routine user compromise, including an offline or otherwise isolated copy where appropriate to the service. Set retention and recovery targets, monitor failed jobs and test restoration. Cloud synchronisation and recycle bins are useful features but should not be assumed to meet your recovery requirements.

Keep a register of internet-facing services and supplier connections. Remove unneeded access; restrict remote administration and record authorised changes. Protect logs from ordinary modification, limit sensitive content and decide who reviews alerts. Technical settings depend on your actual products and should be tested before rollout.

5. Run a proportionate control calendar

Daily or each working shift: review critical security alerts, failed backup jobs, unusual privileged access and payment-change requests. Weekly: review unresolved vulnerabilities, failed updates, stale incidents and restore-test actions. These are suggested operating frequencies; adjust to risk, coverage and contractual requirements.

Monthly: review privileged accounts, external sharing, suppliers with access and expiring exceptions. Quarterly: restore a representative service and rehearse an incident with its business owner. At least annually and after material change: review the risk register, business continuity plan, training and this manual. Record evidence and overdue actions rather than simply ticking "done".

6. Handle incidents and reporting decisions

Treat suspected account takeover, ransomware, significant data exposure, payment fraud or safety-related disruption as urgent. Start a timeline, assign the incident lead and use a trusted communication channel. Distinguish confirmed facts from hypotheses. Preserve relevant logs and messages with access controls; do not upload an evidence dump to a public chatbot.

For a UK personal-data breach, the responsible privacy lead must assess risk promptly. ICO guidance says report notifiable breaches without undue delay and, where feasible, within 72 hours of becoming aware. Where a breach is likely to result in high risk to people, notification to affected people is also generally required without undue delay, subject to applicable conditions and exceptions. Record the decision and reasons even when not reporting. Do not wait for a complete forensic report before assessing deadlines. Check sector, contractual and overseas obligations with qualified advice.

Do not assume every IT outage is a reportable personal-data breach, or that every breach can wait 72 hours. A processor should inform its controller without undue delay. Use current ICO guidance for the organisation's actual role. Do not claim the incident is resolved until recovery, access and business validation are documented.

7. Plan the first 30, 60 and 90 days

Days 1-30: approve owners, inventory critical services, close obvious access gaps, verify backups, publish the reporting route and rehearse one scenario. Days 31-60: implement joiner/mover/leaver and supplier controls, test restore dependencies, address prioritised vulnerabilities and validate safe workarounds. Days 61-90: rehearse cross-department response, measure overdue actions, improve alert coverage and approve the next risk-treatment plan.

Track restore tests passed, time to disable departed-user access, overdue critical findings, incident acknowledgement and recovery against agreed objectives. Training attendance alone does not demonstrate safe behaviour. AIT can help build a company-specific control dashboard and approval process; agree its inputs and access before connecting production systems.

Department responsibilities

Assign real names and deputies. A small company may combine roles, but must preserve accountability and approval boundaries.

Leadership and management

Owner: Managing director / risk owner

Routine: Approve risks, funding, accountable owners and accepted exceptions; review unresolved high-impact findings.

Escalate when: Major disruption, suspected data theft, fraud, safety impact or inability to recover.

Evidence: Risk register, decisions, delegated authority and review minutes.

IT and administration

Owner: IT lead / managed service owner

Routine: Manage identity, patches, backups, configurations, asset inventory and alert review; test authorised changes.

Escalate when: Unusual privileged activity, active exploitation, backup failure or loss of visibility.

Evidence: Change tickets, access reviews, restore results and protected event logs.

Finance and procurement

Owner: Finance lead

Routine: Verify supplier bank changes independently, separate payment approval and maintain trusted supplier contacts.

Escalate when: Unexpected payment, urgent account-change request or suspicious executive instruction.

Evidence: Verification notes, approvals and bank incident reference.

HR and people

Owner: HR lead with line manager

Routine: Notify IT of starters, role changes and departures; protect personnel files and deliver role-specific training.

Escalate when: Unplanned departure, inappropriate personnel access or suspected identity misuse.

Evidence: Authorised access requests, completion confirmation and training actions.

Sales and customer service

Owner: Commercial / service lead

Routine: Use approved CRM and sharing routes, verify unusual customer requests and minimise exports.

Escalate when: Customer data sent incorrectly, fraudulent request or suspicious bulk export.

Evidence: Case notes, disclosure decision and approved customer communication.

Operations and production

Owner: Operations / site lead

Routine: Maintain safe manual workarounds, controlled device use, supplier-access windows and critical-service recovery priorities.

Escalate when: Unsafe equipment behaviour, loss of dispatch/control systems or unknown remote access.

Evidence: Shift log, workaround approvals, reconciliation and restart sign-off.

Marketing and website

Owner: Marketing / website owner

Routine: Control publishing and domain accounts, check approved integrations and record website changes.

Escalate when: Unexpected redirect, false content, lost domain control or exposed enquiry data.

Evidence: Publishing approval, version history, access records and recovery proof.

Privacy, legal and suppliers

Owner: Designated privacy / contract lead

Routine: Review data-processing arrangements, supplier access, retention and breach-reporting duties.

Escalate when: Possible personal-data breach, supplier incident or missed contractual notification.

Evidence: Assessment, reporting decision, supplier correspondence and action log.

Business and sector scenarios

Planning scenarios, not assessments of named businesses. Add sector-specific safety, contractual and regulatory requirements before adoption.

Retail and e-commerce

Priorities: Storefront, customer accounts, order records, payment-provider connections and refunds.

Scenario: An administrator account changes checkout links.

Adaptation: Separate publishing/refund rights; preserve a clean site version; verify payment-provider settings. Assess applicable payment obligations with the provider.

Manufacturing

Priorities: Production availability, engineering files, machinery support and safe restart.

Scenario: An office compromise reaches a production-support workstation.

Adaptation: Map IT/OT boundaries with competent engineers; control supplier access; do not scan, patch or disconnect machinery without safety review.

Warehousing and logistics

Priorities: WMS, labels, handhelds, dispatch interfaces and traceability.

Scenario: Dispatch software is unavailable during a busy shift.

Adaptation: Approve a minimal offline dispatch process and reconcile every temporary shipment record after recovery; protect labels and customer addresses.

Professional services

Priorities: Client confidentiality, document sharing, billing and delegated access.

Scenario: A confidential client folder is shared externally.

Adaptation: Review links and client boundaries; use restricted matter/project folders and confirm who can approve external disclosure.

Care and health-related businesses

Priorities: Sensitive records, appointment continuity and safe delivery of care.

Scenario: A scheduling service outage affects visits.

Adaptation: Agree safe fallback and welfare escalation with the responsible care lead. Specialist health, safeguarding and sector obligations require additional assessment.

Construction and field services

Priorities: Mobile devices, contractor access, drawings and supplier payments.

Scenario: A technician loses a phone containing job information.

Adaptation: Use managed access, minimal offline data and a tested lost-device process; keep current drawings available through controlled routes.

Hospitality

Priorities: Booking systems, guest information, tills and staff turnover.

Scenario: Guest Wi-Fi shares access with a business device network.

Adaptation: Separate guest and business services, review temporary staff access and arrange a safe booking/till fallback with providers.

Education and training

Priorities: Learner information, shared devices, safeguarding and continuity of teaching.

Scenario: An account exposes a learner document set.

Adaptation: Separate staff/learner permissions, minimise shared-device persistence and involve the safeguarding/privacy leads where relevant.

Charities and community organisations

Priorities: Donor and beneficiary data, volunteer access and donation accounts.

Scenario: A volunteer retains access after leaving.

Adaptation: Assign an owner for each platform, expire temporary access and verify changes to donation destinations through two trusted people.

Software and digital agencies

Priorities: Source code, secrets, deployment pipelines and customer environments.

Scenario: A repository or build credential is exposed.

Adaptation: Revoke and rotate credentials, assess use and affected deployments, protect CI/CD access and separate customer environments.

Remote and hybrid teams

Priorities: Identity, laptops, home networks, cloud sharing and remote support.

Scenario: A fake helpdesk call persuades a user to install remote access.

Adaptation: Publish a trusted support-verification route; restrict remote tools and test response when the user is away from an office.

Multi-site SMEs

Priorities: Consistent identity, local ownership, WAN dependencies and cross-site recovery.

Scenario: One site loses connectivity while central systems remain healthy.

Adaptation: Give each site a deputy and safe offline procedure, define local versus central incident authority and test inter-site dependencies.

Step-by-step procedures

01. Joiner, role change and leaver

Owner: Line manager + HR + IT

Start when: A person starts, changes duties or leaves.

1. Manager requests named role-based access and an end date for temporary rights.

2. IT grants minimum approved access; deliver sign-in and reporting guidance.

3. On role change, remove superseded rights as well as adding new rights.

4. On departure, disable access at the agreed time, revoke active sessions/tokens where supported, transfer ownership and recover devices.

5. Check shared accounts, supplier portals, delegated mail and recovery contacts.

Evidence: Approved request and timestamped completion checklist.

Completion / handoff: Manager confirms retained business records and removal of unnecessary access.

02. Phishing or suspicious message

Owner: User + IT triage lead

Start when: Unexpected link, attachment, credential request or urgent instruction.

1. Do not open, reply or forward attachments to colleagues; report by the approved route.

2. Verify the request using an independently known channel.

3. Tell IT whether any link was opened, data entered or file executed.

4. IT preserves relevant evidence and checks related users/messages; contain affected access if indicated.

5. Use the relevant takeover, malware or fraud playbook if activity occurred.

Evidence: Message reference, time and actions actually taken; handle content as untrusted.

Completion / handoff: Scope reviewed, affected people advised and protective actions verified.

03. Suspected account takeover

Owner: IT incident lead

Start when: Unrecognised sign-in, new MFA method, forwarding rule or sent message.

1. Use a trusted device and contact route; assign the incident lead.

2. Preserve relevant identity/mail audit information.

3. Restrict affected access, revoke sessions/tokens and reset credentials through approved recovery.

4. Review MFA methods, recovery details, forwarding rules, delegated access and connected applications.

5. Assess downstream services and data exposure; restore only after validating the trusted account state.

Evidence: Audit timeline, access changes, affected services and privacy assessment.

Completion / handoff: IT and account owner confirm controlled access and follow-up monitoring.

04. Malware or ransomware

Owner: Incident lead + IT; site safety lead where relevant

Start when: Encryption notice, malicious execution or multiple unusable systems.

1. Stop using the affected device; contact the incident team through a trusted channel.

2. IT isolates affected endpoints/network access using approved controls. For operational equipment, coordinate safety before intervention.

3. Do not wipe, reinstall or power-cycle systems as an improvised fix; follow specialist direction and preserve evidence.

4. Identify scope, access path and backup integrity. Engage qualified response support when needed.

5. Recover into a clean controlled environment, validate service/data and monitor before reconnection. Do not negotiate or pay a demand under this general manual.

Evidence: Incident timeline, containment decisions, clean restore tests and business sign-off.

Completion / handoff: Cause addressed sufficiently for safe operation; restored data and access validated.

05. Supplier payment change or fraud

Owner: Finance lead

Start when: Changed bank details, suspicious payment or urgent executive request.

1. Pause the change/payment pending independent verification.

2. Call an established supplier contact using trusted records, not details in the message.

3. Record verification and separate approval where practical.

4. If funds may have gone to an attacker, contact the bank immediately through a trusted route and preserve records.

5. Assess account compromise and reporting obligations with the incident/privacy leads.

Evidence: Verification notes, approver and bank reference; no credentials in the log.

Completion / handoff: Payment destination confirmed or blocked and investigation/recovery actions assigned.

06. Lost or stolen device

Owner: User + IT + privacy lead

Start when: Missing laptop, phone, removable media or printed sensitive material.

1. Report promptly, including last known possession and likely data/access.

2. IT restricts access and invokes managed lock/wipe only under the approved process.

3. Assess encryption, session state, stored data and downstream access; do not assume encryption settles the whole risk.

4. Preserve management records and assess personal-data implications.

5. Replace/re-enrol safely and validate removal of old device trust.

Evidence: Device identifier, times, management actions and risk assessment.

Completion / handoff: Access controlled, reporting assessed and replacement authorised.

07. Accidental data disclosure

Owner: Privacy lead + data owner + IT

Start when: Wrong recipient, exposed sharing link or unapproved upload.

1. Report immediately; do not conceal the mistake or send further sensitive information.

2. Remove inappropriate access where possible and preserve evidence of what was exposed.

3. Establish data types, recipients, exposure window and whether access occurred.

4. Assess risk and reporting deadlines; ask for secure deletion through an approved route without assuming a request proves deletion.

5. Correct sharing controls and support affected people as appropriate.

Evidence: Disclosure record, assessment, notification decisions and mitigation.

Completion / handoff: Exposure contained, responsibilities discharged and corrective actions assigned.

08. Critical service or supplier outage

Owner: Service owner + incident lead

Start when: Email, SaaS, network or operational service is unavailable.

1. Confirm impact and check official supplier status using a trusted route.

2. Activate the approved manual/alternative process; avoid duplicate orders and unsafe shortcuts.

3. Keep a minimum reconciliation record and give users factual updates.

4. Coordinate supplier recovery and validate restored service with a representative workflow.

5. Reconcile temporary records and confirm that access/logging protections remain active.

Evidence: Impact, supplier references, workaround transactions and validation.

Completion / handoff: Business owner accepts service and reconciled backlog.

09. Website or domain compromise

Owner: Website owner + IT

Start when: Unexpected redirects, content, DNS changes or lost publishing access.

1. Escalate and preserve hosting/domain audit records.

2. Restrict compromised access and coordinate with the registrar/host through trusted support.

3. Where needed, suspend affected content through the authorised owner; retain clean backups.

4. Review integrations, secrets, customer forms and possible exposure.

5. Restore a verified version, rotate affected credentials and test public routes and enquiry handling.

Evidence: Affected URLs, change history, recovery version and tests.

Completion / handoff: Domain/site control verified and user impact assessed.

10. Supplier remote-access request

Owner: System owner + IT; operations approval for machinery

Start when: Vendor requests remote access or elevated permissions.

1. Verify identity, purpose, target, time window and contract scope.

2. Approve named least-privilege access; avoid shared permanent admin credentials.

3. Record the session or relevant audit events consistent with privacy obligations.

4. Monitor agreed work, review changes and revoke temporary access at completion.

5. Validate the business system and record exceptions.

Evidence: Access approval, session/change reference and revocation confirmation.

Completion / handoff: Owner accepts work and temporary rights are removed.

11. Patch and configuration change

Owner: IT change owner + business service owner

Start when: Security update, exposed weakness or planned configuration change.

1. Identify affected assets, exploit risk and business impact.

2. Assign priority and deadline based on actual exposure; urgent exploitation may need accelerated action.

3. Prepare backup/rollback and test on representative systems; include OT safety constraints.

4. Approve and deploy in a controlled window with status monitoring.

5. Verify installation, access and application behaviour; document residual risk or failure.

Evidence: Change record, approval, version/setting verification and rollback readiness.

Completion / handoff: Security objective and business function verified or rollback completed.

12. Restore test and business recovery

Owner: IT restore lead + process owner

Start when: Scheduled test or incident recovery authorisation.

1. Choose a representative dataset/service and define success without overwriting production.

2. Check dependencies and retrieve an authorised backup into an isolated test location.

3. Validate integrity, access restrictions and business transactions with the data owner.

4. Measure achieved recovery time and data gap against agreed objectives.

5. Protect/delete test copies appropriately; fix failed dependencies and schedule retest.

Evidence: Backup reference, restore timestamps, tests and owner approval.

Completion / handoff: Objective met with evidence, or failure tracked with a named action and retest.

Records, approvals and maintenance

Use the companion forms to record company/case reference, owner and time zone, scope/trigger, verified facts, actions, approvals, completion and next review. Preserve original evidence in a restricted approved location; use references rather than copying sensitive material unnecessarily.

Company adoption checklist

- Define legal entities, sites, systems, information categories and exclusions.

- Assign accountable owners, deputies and escalation contacts, including agreed coverage hours.

- Agree retention, access, response objectives, budgets and stop conditions.

- Test representative workflows, exceptions, recovery and approval boundaries.

- Approve a version, train users, record evidence and set the next review date.

Urgent, significant and routine work

Urgent: suspected active compromise, sensitive-data exposure, fraud, safety risk or critical loss of service. Contact the named lead immediately through a trusted route. Significant: contained material disruption or weakness, with a coordinated owner and deadline. Routine: low-impact requests tracked to closure. Define actual response times and reclassify if impact changes.

The manual and AIT contact form are not emergency channels. Do not delay bank, safety or incident escalation while completing a form.

Custom implementation with AIT Technology

We can adapt this manual to your organisation and departments, map existing processes and build bespoke software, controlled AI workflows, integrations, approval queues and practical dashboards. Begin with discovery, agree scope and tests, implement reversibly, validate with users, and agree ongoing ownership and support separately.

Sources and limitations

Sources checked 18 November 2026. This is original AIT operational guidance. Suggested roles, frequencies, templates and workflows must be tailored; they are not verbatim official requirements. Linked guidance may change. Regulated or safety-critical use requires appropriate specialist assessment.

NCSC: small organisations guide to cyber security

https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security

NCSC: 10 Steps to Cyber Security

https://www.ncsc.gov.uk/collection/10-steps

NCSC: incident management

https://www.ncsc.gov.uk/collection/incident-management

NCSC: supply chain security

https://www.ncsc.gov.uk/collection/supply-chain-security

ICO: personal-data breach reporting

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Discuss a tailored implementation: https://aittech.co.uk/contact/