1. Incident summary

Business Microsoft 365 / Office 365 accounts - use UTC or state the time zone.

Blank fillable template. Save a local copy and confirm entries persist in your PDF reader. Use an access-controlled continuation record for longer findings. Do not enter secrets.

Incident reference

Prepared by / role

Organisation / controller

Tenant ID / primary domain

Affected account / account type

Incident owner / trusted contact

Discovered at (date, time, zone)

Organisation aware at (date, time, zone)

Investigation window: start

Investigation window: end / ongoing

Trigger, reported symptoms and initial status

Evidence location / export IDs / who collected / time / integrity record

Confirmed facts, working hypotheses and important unknowns

2. Containment and identity

Record who acted, when, result and evidence reference. Not every action fits every tenant.

Work from a trusted admin account and device. Preserve evidence alongside urgent containment. Keep compromised access blocked if unauthorised methods or activity return.

Block sign-in / revoke sessions: action, operator, time, verification and app session limits

Password reset: cloud / AD / federation source, time and secure handover (no passwords)

MFA methods: before/after, unrecognised methods removed, passkeys / TAP review, trusted re-registration

App passwords / app consent / roles / devices / other identity access: findings and actions

Recurrence or repeated resets: what returned, when, suspected access path and escalation owner

Re-register MFA is not proof all authentication methods were removed. Follow Microsoft hybrid-specific guidance if a double AD password reset is required; it is not a universal cloud-account rule.

3. Mailbox rules and access

Preserve relevant settings before remediation. Reference protected exports for detail.

Inbox rules review: mailbox, hidden rules checked, collection time and export reference

Rule 1: name / ID; conditions; action / destination; enabled; time / evidence; disposition / operator

Rule 2: name / ID; conditions; action / destination; enabled; time / evidence; disposition / operator

Rule 3: name / ID; conditions; action / destination; enabled; time / evidence; disposition / operator

Mailbox-level forwarding / delegation / other mail access: findings, changes and evidence

Further rules, audit history, gaps and continuation record reference

4. Messages and exposure

Record counts with definitions. Unknown is a valid finding; do not substitute zero.

Trace window / time zone

Data source / query / export reference

Distinct messages: count / ID method

Recipient or event rows: count / meaning

Confirmed malicious messages / unknown

Delivered / failed / other: count basis

Distinct internal recipients / method

Distinct external recipients / method

Counting method, legitimate mail excluded, estimates, duplicates and incomplete results

Mailbox read / sync / export; files / other accounts: evidence, scope and uncertainty

Suspected fraud / exposed information / affected people; immediate protective actions

Sent Items alone does not establish activity. Message trace records can include multiple recipient rows, events, expansion and forwarding for a message. Keep the raw evidence securely.

5. UK GDPR decision record

Assign a controller decision-maker. Use current ICO guidance and specialist advice as needed.

Controller / processor and responsible lead

Awareness time / 72-hour deadline (zone)

Personal data categories / sensitivity; people and records affected (approximate or unknown)

Confidentiality / integrity / availability impact; likely consequences and risk to people

ICO notification decision, rationale, decision-maker, time; delay reasons / phased updates if needed

Affected people: high-risk assessment, communication decision, rationale, owner and time

Processor to controller notification; ICO / people communications: times and reference numbers

Evidence gaps, next review time and decision owner

Assess notification without undue delay. A notifiable breach should reach the ICO within 72 hours of awareness where feasible. Do not wait for a completed forensic investigation. Keep the breach decision record even if no notification is made.

6. Recovery and closure

Record the current position, not an unsupported assurance that nothing was accessed.

Root cause / confidence; evidence supporting or limiting the conclusion

Restoration checks: trusted identity, authentication, devices, access and mailbox settings; who / when

Monitoring plan: scope, owner, review date, recurrence indicators and escalation route

Outstanding remediation / communications / contractual duties: action, owner and due date

Recovery approval / date

Review or closure date / status

Evidence retention, access restrictions and continuation record references

Official guidance and detailed procedures:

Microsoft: compromised email account

Microsoft: user authentication methods

Microsoft: message trace

ICO: personal data breaches

Template reviewed 18 October 2026. Operational aid; not a legal determination.