INCIDENT TRIAGE / 01 OF 02

Incident response checklist

Use when there are signs of unauthorised access, suspicious changes or possible data exposure. Involve a qualified responder.

- [ ] **01 Nominate a lead and safe contact route**

  Record the decision maker, hosting contact and qualified responder. Use a trusted device and communication route if current accounts or systems may be compromised. Do not rely on a suspected account for incident coordination.

- [ ] **02 Record what was actually observed**

  Capture the time and time zone, system, observer and original alert. Separate confirmed observations from assumptions. Do not claim a specific CVE caused the incident without evidence.

- [ ] **03 Agree immediate containment**

  Work with the owner, host and responder to restrict access, isolate affected services or take them offline where necessary. Balance urgent harm reduction with evidence preservation; record approval and business impact.

- [ ] **04 Preserve original evidence**

  Protect relevant logs, authorised snapshots, configuration and alerts. Record collection time, method, custodian and integrity information. Do not run cleanup tools, delete suspicious files or overwrite evidence before advice.

- [ ] **05 Assess the scope**

  Identify affected accounts, sites, databases, secrets, integrations and related systems. Establish the possible exposure window and known gaps. Check for unauthorised persistence and activity beyond the visible website.

> **Routine support has limits**
>
> Bytova's everyday computer-support appointments exclude active incidents and forensic investigation. A PHP update alone does not remove an existing backdoor, restore data integrity or prove that compromise did not occur.

Independent educational guidance. No security guarantee or authority endorsement.

Sources: UK NCSC guidance (21 Oct 2026)

INCIDENT RESPONSE / 02 OF 02

Investigate. Recover. Keep a decision record.

The response lead and qualified adviser should agree each consequential action. Preserve both evidence and uncertainty.

06 Investigate with controlled access

Correlate web, PHP, authentication, deployment and application evidence. Investigate new administrators, unexplained files or jobs and unexpected outbound traffic. Retain original records and avoid publishing customer evidence.

07 Plan a trusted recovery

Determine the likely entry point and persistence. Agree whether to rebuild from a trusted baseline or restore an independently assessed clean backup. Patch the relevant runtime, application and dependencies before reconnecting.

08 Rotate exposed access safely

After containment, use a trusted device to rotate affected credentials, tokens and application secrets with the responsible owners. Review dependent services and revoke unnecessary access; preserve relevant access evidence first.

09 Validate before return to service

Confirm the fixed running runtime and replaced workers. Check data integrity, essential functionality and working logs. Restore access in stages with a named owner and a clear route back to containment if needed.

10 Communicate, review and follow up

Use approved factual messages. Record reporting or notification decisions with the responsible professional adviser. Track unresolved risks and monitoring, then review causes, recovery lessons and any changes to access or backups.

What this checklist cannot decide

It cannot determine legal notification obligations, establish attribution or certify a clean system. An absence of obvious indicators is not proof that no compromise occurred. Obtain appropriate incident, legal and privacy advice for your circumstances.

Independent educational guidance. No security guarantee or authority endorsement.

Sources: UK NCSC guidance (21 Oct 2026)