CASE RECORD / 01 OF 02

Security incident record

Printable blank template. Keep in a protected case folder. Record observations separately from interpretation; exclude passwords and unnecessary personal data.

Case ID / incident lead / contact route

Affected service / owner / hosting environment

First observed: date, time and time zone / observer / alert source

Confirmed observations and evidence references

What was directly seen? Where is the original evidence retained?

Hypotheses, unknowns and scope gaps

What is suspected, and what still needs to be verified?

Immediate containment / authorisation / business impact

Who approved the action, when, and what effect did it have?

Independent educational guidance. No security guarantee or authority endorsement.

Sources: UK NCSC guidance (21 Oct 2026)

CASE RECORD / 02 OF 02

Evidence, decisions and follow-up

Continue with the same case ID. Retain original evidence; use protected references rather than copying sensitive material into this form.

Case ID / person completing this page / date and time zone

Evidence custody record

Evidence reference / integrity	Collected: time + zone / method	Custodian / access or transfer

Action and decision log

Time + zone / action	Authoriser / rationale / evidence	Result / uncertainty / owner

Recovery validation / reporting decision references / approver

Outstanding actions / owner / due date / next review

Independent educational guidance. No security guarantee or authority endorsement.

Sources: UK NCSC guidance (21 Oct 2026)