THE FIRST HOUR

A calm response card for a suspicious login, compromised mailbox, ransomware note, lost device, or fraudulent payment.

Safety first: protect people and essential operations. Do not power off, wipe, delete, or “clean up” evidence unless the authorised technical responder tells you to.

1

STOP THE SPREAD

Disconnect the affected device from Wi-Fi/network if safe. Stop suspicious payments or account changes. Do not keep clicking.

2

USE THE CONTACT SHEET

Call the internal incident lead and the authorised IT/security contact. Use known numbers, not information from the suspicious message.

3

CALL THE INSURER / BREACH LINE

When cyber insurance may apply, follow the policy’s notice and vendor instructions before hiring outside responders. Coverage rules vary.

4

PRESERVE EVIDENCE

Keep emails, headers, screenshots, timestamps, files, device names, and notes. Do not delete the message or reset everything blindly.

5

CONTAIN MONEY + ACCOUNTS

If money moved, call the bank immediately for a fraud hold/recall. If credentials were entered, use the authorised reset and session-revocation process.

6

DECIDE + COMMUNICATE

Leadership decides on client, employee, privacy, legal, law-enforcement, and regulator notifications. Communicate facts calmly; do not speculate.

FILL THIS IN BEFORE THE INCIDENT

Your first-hour contact sheet

Print this page, fill it in, and store a copy somewhere the team can reach when email or the shared drive is unavailable.

Incident lead
Name / mobile / alternate

Executive decision-maker
Name / mobile

IT / managed-service provider
Company / emergency number / account reference

Cyber insurer / breach line
Carrier / policy number / 24-hour number

Bank fraud line
Bank / number / business account reference

Privacy / legal adviser
Name / number

Communications / client lead

INCIDENT NOTES

Record: what happened, when it was first noticed, affected people/devices/accounts, and actions already taken.