FREE RESOURCE / XBITIUM SECURITY

Incident Response Plan Template

What to do in the first hour, when nobody is thinking clearly.

An incident response plan is not for your calm, competent self. It is for the version of you at 2am who has just discovered the files are encrypted and whose adrenaline has erased the ability to think. This template is written for **that** person. Fill in the contacts today, print the action card, and put it somewhere you will find it when the screens are locked.

FILL THIS IN NOW, NOT LATER

The blanks below are useless if you complete them *during* an incident. Spend fifteen minutes filling in the names and numbers today. That fifteen minutes is the entire point of this document.

The first 60 minutes (print this page)

If you suspect a breach, ransomware, or a compromised account, work through these in order. Do not skip step 1.

Done	Control	Why this one matters
☐	**Do NOT turn the machine off — disconnect it from the network instead**	Powering off can destroy evidence needed to understand the attack. Unplug the network cable or disable WiFi to contain it while preserving the scene.
☐	**Call your incident lead and IT contact (numbers below)**	Get the right people engaged immediately. Do not try to be a hero alone.
☐	**Write down what you saw and when, before you forget**	Time, what was on screen, what was clicked. Memory degrades fast under stress.
☐	**Do NOT pay, click, or reply to any ransom or attacker message yet**	Decisions made in panic are usually wrong. Get advice first.
☐	**Preserve, do not clean up**	Resist the urge to delete or fix things. You may be destroying the evidence that explains how they got in.

Emergency contacts

Incident lead	*[Name, mobile — the person who runs the response]*
IT / MSP support	*[Company, 24/7 number]*
Security partner	*[e.g. Xbitium, contact]*
Cyber insurance	*[Insurer, policy number, claims hotline]*
Legal counsel	*[Name, number]*
Bank fraud line	*[For invoice or wire fraud]*
Key staff to notify	*[Owner, operations lead]*

The six phases

Based on the widely used SANS / NIST incident-handling model, translated out of jargon.

1. Prepare (before anything happens)

Fill in this plan. Ensure backups exist and have been tested. Confirm your insurance is active and that you know what it requires. Make sure staff know how to report a problem.

2. Identify (is this real?)

Confirm something is actually wrong and record what you know: which systems, which accounts, what symptoms, and when it started. Not every alert is an incident — but treat a credible suspicion seriously.

3. Contain (stop the bleeding)

Limit the damage. Disconnect affected machines from the network (do not power off). Disable compromised accounts. Preserve evidence. The goal is to stop the spread while keeping the information you will need to understand it.

4. Eradicate (remove the cause)

Once contained, remove the attacker's access and foothold: malware, unauthorised accounts, changed settings, planted backdoors. Do not rush to restore before you are confident the cause is gone, or you will simply be reinfected.

5. Recover (get back to work, carefully)

Restore systems from known-clean backups, reset affected credentials, and watch closely for any sign the attacker returns. Bring things back in a controlled way, not all at once.

6. Learn (so it does not happen twice)

Within two weeks, write down what happened, how they got in, what worked in your response, and what did not. Fix the root cause. A breach you learn nothing from is a breach you have paid for twice.

Notification — who you may be legally required to tell

Depending on what data was involved and where your customers live, you may be legally obligated to notify affected individuals, regulators, or authorities within a set time. Confirm your obligations with legal counsel **before** an incident, so you are not researching breach-notification law during one.

- Affected customers or patients — often within a defined number of days
- State authorities — most US states have breach-notification laws
- Industry regulators — for example HIPAA for health data
- Your cyber-insurance carrier — usually required promptly to keep coverage valid