

Incident Response Plan Template

For Jamaican organizations. Prepared by Syxel Technologies Limited.

How to use this template

This template gives you a complete starting point for a cybersecurity incident response plan. Delete this page before you adopt it.

- Replace everything in [square brackets] with your own details, and delete examples and sections that do not apply to you.
- Name a person, and a deputy, for each role in section 4. In a small organization one person may hold more than one role, but every role needs a named owner.
- Agree the severity levels in section 5 with management, including how quickly each level must be escalated.
- Fill in the emergency contact sheet in Appendix A now, before you need it. Include your IT provider, insurer and bank, with after-hours numbers.
- Decide who your Data Protection Officer or privacy lead is, and make sure they know about the 72-hour reporting requirement in section 13.
- Print the plan and the appendices and keep copies off site. During an incident your email, file server or power may not be available.
- Test the plan with a tabletop exercise (section 19) within [3] months of adopting it, then at least once a year.

This template is general guidance, not legal advice. It was prepared by Syxel Technologies Limited with the Jamaica Data Protection Act, 2020 in mind. Agency names and reporting channels were checked when the template was written, so confirm them before you rely on them. For help adapting the plan or running a tabletop exercise, contact sales@syxeltech.com.

[Organization] Cybersecurity Incident Response Plan

Plan owner	[Role, e.g. IT Manager or Operations Manager]
Approved by	[Name, role]
Version	[1.0]
Effective date	[Date]
Last tested	[Date of last tabletop exercise]
Next review	[Date, 12 months after the effective date]
Where copies are kept	[e.g. shared drive, printed copy at reception safe, printed copy with the Incident Lead off site]

1. Purpose

This plan sets out how [Organization] prepares for, detects, responds to and recovers from cybersecurity incidents. Its aims are to limit harm to our customers, staff and operations, to restore normal service quickly and safely, to protect evidence, and to meet our legal duties, including the duty under the Data Protection Act, 2020 (the "Act") to report certain breaches to the Information Commissioner within 72 hours.

2. Scope

This plan applies to:

- all information systems, networks, devices, cloud services and data that [Organization] owns, manages or uses, including systems run for us by IT providers and other third parties;
- all employees, contractors, interns and volunteers, who must report suspected incidents as set out in section 7;
- all of our locations: [list offices, branches and sites].

Physical emergencies such as fire, hurricanes and flooding are covered by our [business continuity or disaster recovery plan]. Where a physical event and a cyber incident happen together, the Incident Lead coordinates with the person responsible for that plan.

3. Definitions

Term	Meaning
Security event	Something observed on a system or network that might indicate a problem, such as a failed login, an antivirus alert or a suspicious email. Most events are not incidents.
Incident	An event that harms, or threatens to harm, the confidentiality, integrity or availability of our information or systems. Examples: ransomware, a compromised email account, a stolen laptop, fraudulent payment instructions, or personal data sent to the wrong person.
Personal data	Information about a living person who can be identified from it, directly or indirectly, such as a name, address, TRN, account number, photo or voice recording.
Sensitive personal data	Personal data the Act protects more strictly, such as health, genetic or biometric data, and information about criminal offenses. See the Act for the full definition.
Personal data breach	A security breach that affects, or may affect, personal data: for example, personal data that is lost, stolen, destroyed, altered, disclosed or accessed without authorization.
Containment	Steps that stop an incident from spreading or causing more harm.
Eradication	Removing the cause of the incident, such as malware, attacker access or a weakness that was exploited.
Recovery	Restoring systems and data to normal, secure operation.
Evidence	Logs, devices, emails, files, screenshots and records that show what happened and may be needed for investigation, insurance or legal action.

4. Roles and responsibilities

The incident response team is made up of the roles below. Contact details for each person and their deputy are in Appendix A. If a role holder is unavailable, their deputy acts with the same authority.

Role	Held by	Responsibilities
Incident Lead	[Name, role]. Deputy: [name, role]	Takes charge of the response. Confirms the severity level, assembles the team, assigns tasks, keeps the incident log up to date, and is the single point of coordination until the incident is closed.

Role	Held by	Responsibilities
Technical Lead	[Name, role, or IT provider]. Deputy: [name]	Investigates what happened and how. Directs containment, eradication and recovery, preserves technical evidence, and works with the IT provider and any outside specialists.
Communications Lead	[Name, role]. Deputy: [name]	Prepares all messages to staff, customers, partners and the media, gets them approved, and is the only person, with the Management Sponsor, who speaks to the media.
Data Protection Officer or privacy lead	[Name, role]. Deputy: [name]	Decides whether personal data is affected, assesses the risk to the people concerned, prepares and submits the report to the Information Commissioner within 72 hours, and advises on notifying affected people.
Management Sponsor	[Name, e.g. Managing Director or CEO]	Approves major decisions: shutting down systems, spending, engaging outside specialists, notifying regulators, customers and the media, and dealing with any ransom demand. Signs off the closure of Severity 1 and 2 incidents.
Log Keeper	[Name, role]	Records actions, decisions and times in the incident log (Appendix C) so the Incident Lead can focus on the response.
All staff	Everyone covered by this plan	Report anything suspicious straight away, follow instructions from the Incident Lead, and do not discuss the incident outside the response team unless authorized.

5. Severity levels

The Incident Lead assigns a severity level during triage and reviews it as more is learned. If in doubt, choose the higher level. Any incident that may involve personal data is treated as at least Severity 2 until the Data Protection Officer decides otherwise.

Level	Description	Examples	Who is told, and how fast
Severity 1: Critical	Core operations stopped or at serious risk, large amounts of personal or sensitive data exposed, or money lost.	Ransomware spreading across systems; a fraudulent payment sent; a customer database stolen; a payment or core banking system down.	Incident Lead, Management Sponsor and Data Protection Officer [immediately]. Full team works until the incident is contained.

Level	Description	Examples	Who is told, and how fast
Severity 2: High	Important systems or a whole department affected, or personal data of a number of people may be exposed.	A compromised administrator account; a staff email account used to send phishing to customers; a stolen unencrypted laptop with customer files.	Incident Lead and Data Protection Officer [within 1 hour]. Management Sponsor [within 4 hours].
Severity 3: Medium	Limited impact, confined to one user or device, with no sign of data being accessed.	Malware found on one laptop; one email account compromised with no sign of data access or onward phishing.	Incident Lead [within 1 working day].
Severity 4: Low	Attempted attack that was blocked, or a minor policy breach with no data exposed.	A phishing email reported and not clicked; repeated failed login attempts that were blocked.	Recorded by [IT or the Incident Lead]. Reviewed [monthly] for patterns.

6. Phase 1: Preparation

Preparation is what makes the rest of this plan work. [Plan owner] makes sure that:

- ☐ every role in section 4 has a named person and a deputy, and they know what is expected of them;
- ☐ the emergency contact sheet (Appendix A) is complete, checked every [6] months, and printed and stored off site;
- ☐ we keep an up-to-date list of our key systems, the data each one holds, who supports it and how to restore it;
- ☐ we know where personal data is held and which systems hold sensitive personal data;
- ☐ backups of key systems are taken [daily], at least one copy is kept offline or cannot be altered, and restores are tested [every quarter];
- ☐ logging is turned on for firewalls, servers, email and cloud services, and logs are kept for at least [90 days];
- ☐ multi-factor authentication is turned on for email, remote access, cloud services and administrator accounts;
- ☐ our IT provider contract says what help they give during an incident, including after hours;
- ☐ we know what our cyber insurance policy covers, how to notify the insurer and whether we must use its approved providers;
- ☐ staff are trained to recognize and report incidents, and know the reporting channels in section 7;
- ☐ we have a way to communicate if email is down or compromised, such as a phone tree or a separate messaging group [describe];
- ☐ the plan has been tested with a tabletop exercise in the last [12] months (section 19).

7. Phase 2: Detection and reporting

Incidents are detected by staff, customers, security tools, our IT provider, banks or outside parties. Anyone who suspects an incident must report it straight away to [IT help desk or Incident Lead, with phone number and email]. Outside working hours, call [after-hours number]. If you think your email account is compromised, report by phone, not email.

Report anything like this:

- a ransom note, files that will not open or have strange new names;
- a click on a suspicious link or attachment, or entering your password on a suspicious page;
- emails sent from your account that you did not send, or new forwarding rules you did not create;
- a request to change a supplier's or employee's bank details, or an unusual request for payment;
- a lost or stolen laptop, phone, USB drive or paper files;
- personal data sent to the wrong person or posted in the wrong place;
- unexpected pop-ups, programs, account lockouts, or a computer that suddenly runs very slowly;
- a customer or supplier telling you they received a strange message from us.

When you report, do not:

- switch off an affected computer, unless told to. Disconnect it from the network instead (unplug the network cable and turn off Wi-Fi);
- delete suspicious emails or files, run your own clean-up tools, or try to investigate yourself;
- contact the attacker, reply to a ransom note or pay anything;
- discuss the incident on social media, with the media or with anyone outside the response team.

You will not be penalized for reporting an honest mistake promptly. Reporting quickly is the single biggest thing you can do to limit the harm.

8. Phase 3: Triage

The person who receives the report contacts the Incident Lead. Within [1 hour] of a report, the Incident Lead, with the Technical Lead, works through the following:

- ☐ Open an incident record and give it a reference number [format, e.g. IR-2026-001]. Start the incident log (Appendix C).
- ☐ Get the facts from the person who reported it, using the incident report form (Appendix B).
- ☐ Confirm whether this is a real incident or a false alarm. If it is a false alarm, record it and close it.
- ☐ Work out what is affected: which systems, accounts, devices, locations and data.
- ☐ Decide whether the incident is still happening or spreading.

- ☐ Decide whether personal data may be involved. If it may be, tell the Data Protection Officer straight away and record the date and time we became aware. The 72-hour deadline for reporting to the Information Commissioner runs from this point (section 13).
- ☐ Assign a severity level (section 5) and escalate as that level requires.
- ☐ Decide whether outside help is needed now: IT provider, insurer, bank, or incident response specialists.
- ☐ Decide how the team will communicate. If email or the network may be compromised, use [phone or separate messaging group].

9. Phase 4: Containment

The goal of containment is to stop the damage from spreading while keeping evidence. The Technical Lead decides the steps; the Management Sponsor approves anything that will disrupt operations, such as taking a key system offline. The table gives first steps for common incidents.

Incident type	First containment steps
Ransomware	Disconnect affected devices from the network but leave them powered on. Disconnect or protect backups so they are not encrypted too. Disable accounts that may be compromised. Block remote access until it is checked. Do not contact the attackers or pay. Call the IT provider and the insurer.
Compromised email account	Reset the password from a clean device and sign the account out of all sessions. Turn on multi-factor authentication. Remove any forwarding or mailbox rules the user did not create. Check sent items for phishing sent to contacts, and warn them if needed.
Payment fraud or changed bank details	Call the bank's fraud line immediately to try to stop or recall the payment. Freeze further payments to the affected supplier. Confirm any change of bank details by calling a phone number you already have on file, not one in the email. Keep the emails as evidence.
Lost or stolen device	Lock or wipe the device remotely if possible. Change passwords for accounts used on it. Find out whether it was encrypted and what data it held. Report a theft to the police and get a reference number.
Personal data sent to the wrong person	Recall the email if possible. Ask the recipient to delete it and confirm in writing that they have done so and not shared it. Tell the Data Protection Officer.
Website defaced or compromised	Take the site offline or replace it with a maintenance page. Keep a copy of the compromised site for evidence. Change administrator and hosting passwords, and check for added user accounts.
Malware on one device	Isolate the device from the network. Have the Technical Lead check whether other devices show the same signs.

Incident type	First containment steps
Misuse by a staff member or contractor	Suspend the person's access, preserve their account and logs, and involve [HR] and a legal adviser before taking further steps.

Record every containment action in the incident log, with the time and who did it.

10. Phase 5: Eradication

Once the incident is contained, the Technical Lead removes its cause. This normally includes:

- ☐ identifying how the attacker got in, such as a phishing email, a weak or reused password, an unpatched system or an exposed remote access service;
- ☐ removing malware, unauthorized accounts, remote access tools, forwarding rules and scheduled tasks the attacker created;
- ☐ rebuilding affected systems from clean, known-good sources where there is any doubt that cleaning is enough;
- ☐ resetting passwords for affected accounts, administrator accounts and service accounts, and revoking access tokens and keys that may be exposed;
- ☐ fixing the weakness that was exploited, such as applying patches, closing exposed services or tightening firewall rules;
- ☐ checking other systems for the same weakness or signs of the same attacker.

11. Phase 6: Recovery

Recovery returns systems to normal operation safely. The Technical Lead and the owner of each business system agree the order in which systems are restored, starting with [the systems most critical to operations, e.g. payments, customer service, payroll].

- ☐ Confirm the backups to be used were taken before the incident began and are free of malware.
- ☐ Restore systems and data, and check them with the people who use them before returning them to service.
- ☐ Bring systems back in stages, watching for signs that the attacker is still present.
- ☐ Monitor affected systems and accounts closely for at least [30] days after recovery.
- ☐ Tell staff and, where appropriate, customers when services are back to normal.
- ☐ Record what data, if any, could not be recovered.
- ☐ The Incident Lead confirms the incident is resolved, and the Management Sponsor signs off closure for Severity 1 and 2 incidents.

In Jamaica, recovery may coincide with power outages or storm damage. Make sure the systems you restore first have reliable power and connectivity, and follow our [business continuity plan]

where it applies.

12. Phase 7: Post-incident review

Within [10] working days of closing a Severity 1 or 2 incident, the Incident Lead holds a review meeting with the response team and the people affected. Severity 3 incidents are reviewed [monthly as a group]. The review is about improving, not blaming.

- Use the post-incident review form in Appendix E.
- Agree what happened, the root cause, how it was detected and how long each phase took.
- Identify what worked well and what did not, including any part of this plan that was unclear or not followed.
- Agree actions, each with an owner and a due date, and track them to completion.
- Update this plan, the contact sheet and staff training as needed.
- Report the findings and the action plan to [management or the board].

13. Personal data breaches and the Data Protection Act

Under the Act, a data controller must report to the Information Commissioner any security breach that affects or may affect personal data, and any contravention of the data protection standards, within 72 hours of becoming aware of it. The Data Protection Officer is responsible for making this report on behalf of [Organization].

- The 72 hours start when we become aware of the breach, not when the investigation ends. Weekends and public holidays count. The Data Protection Officer records the date and time we became aware in the incident log.
- Do not wait until all the facts are known. The Information Commissioner's online breach report form allows a report to be made in phases: an initial report, follow-up reports and a final report.
- Report through the "Report a Data Breach" form on the Office of the Information Commissioner's official website. The OIC has warned the public about a fraudulent website imitating it, so check that you are on the official site before entering any information.
- Affected people must be notified as required by the regulations. The Data Protection Officer decides, with the Management Sponsor, who must be told, what they are told and how.
- If a service provider that processes personal data for us has a breach, we may still need to report it. Our contracts with these providers should require them to tell us promptly.
- We keep a record of every personal data breach, including those we decide not to report, with the facts, the risk assessment and the reasons for our decision.

In general terms, the report to the Information Commissioner describes:

- who we are, and the contact details of our Data Protection Officer and of any service provider involved;
- what happened, when it happened and when we became aware of it, how it was detected and its likely cause;
- the types of personal data affected, and the approximate number and categories of people affected;
- the likely consequences for the people affected;
- what we have done and plan to do to deal with the breach and reduce the harm, including whether we have reported it to the police;
- whether and how we have notified the people affected.

Our [data breach response checklist] sets out the detailed steps. Breaching the Act's standards or failing to make a required report is an offense, and penalties can be significant, so take legal advice where the position is unclear.

14. Communications

All communication about an incident is coordinated by the Communications Lead and approved by [the Management Sponsor] before it is sent. Messages must be accurate, consistent and free of speculation. Never say that no data was affected until that has been confirmed.

Audience	What to do
Response team	Use [phone or a separate messaging group] if email or the network may be compromised. Share incident details only with people who need them.
Staff	Tell staff what has happened in general terms, what they must do (for example, not to use a system, or to reset a password), and that they must not discuss the incident publicly or on social media. Tell them how to direct customer and media questions.
Customers	Where customers are affected, tell them what happened, what it means for them, what we are doing and what they can do to protect themselves. Give front-line staff a short script and answers to likely questions. Notify people whose personal data is affected as required by the regulations (section 13).
Media	Only [the Communications Lead and the Management Sponsor] speak to the media. Use a holding statement until the facts are confirmed, and do not name suspected attackers or blame others.
Social media	Monitor our pages and mentions. Answer with approved wording only, and move detailed questions to a private channel.

Audience	What to do
Partners, suppliers and regulators	Coordinate with the Incident Lead and the Data Protection Officer so that what we tell each party is consistent.

Holding statement template: "[Organization] is aware of an IT incident affecting [some of our systems]. We acted quickly to contain it and are investigating with [specialist support]. [Services that remain available.] We will share updates at [channel]. Customers with questions can contact [contact details]."

Keep a copy of every message sent, with the date, time and audience, in the incident log.

15. Evidence handling

Evidence may be needed to understand the incident, to support an insurance claim, to report to the authorities and in any legal action. The Technical Lead is responsible for preserving it.

- Do not switch off affected devices unless the Technical Lead says so. Disconnecting them from the network keeps information in memory that may be lost on shutdown.
- Do not run clean-up tools, reinstall systems or delete files before evidence is captured, unless that is needed to stop serious harm. Record it if it happens.
- Export logs from firewalls, servers, email and cloud services as soon as possible. Many services keep logs only for a limited time.
- Photograph ransom notes and error messages. Save suspicious emails as attachments so the full message details are kept, rather than forwarding them.
- Record each item of evidence: what it is, where it came from, who collected it, when, and where it is stored.
- Record every handover of an item of evidence from one person to another (the chain of custody).
- Store evidence securely, with access limited to [named roles]. Work on copies, not originals.
- If legal action or an insurance claim is likely, have forensic copies made by qualified specialists.
- Note the time zone and whether device clocks were accurate, so timelines can be matched.

16. Working with third parties

Third party	When and how to involve them
IT provider	Call [provider] as soon as an incident is suspected, using the after-hours number in Appendix A. Their contract says [what incident support they provide]. Make sure they record what they do in our incident log. If the incident started in the provider's own systems, the Incident Lead takes charge of our response and asks the provider for regular written updates.
Cyber insurer	Notify the insurer as the policy requires, usually as early as possible and before engaging outside specialists. Check whether you must use the insurer's approved forensic, legal or public relations providers. Do not admit liability, and do not pay a ransom or other costs the insurer may cover without its agreement. Keep records of all costs. Policy number: [number].
Bank	If money has been paid to a fraudster, call the bank's fraud line immediately: the chance of recovering funds falls quickly. If online banking credentials may be compromised, ask the bank to block access and review recent payments. Ask the bank what it needs from us, such as a police report.
Software and cloud providers	Report suspected compromise of an account or service, and ask for the logs and help they can provide.
Service providers that process personal data for us	Ask for full details of any breach on their side, and agree who will tell affected people. The Data Protection Officer decides what we must report.
Legal adviser	Involve [firm or adviser] in Severity 1 incidents, in personal data breaches where the reporting position is unclear, and before responding to any ransom or extortion demand.
Incident response specialists	Engage specialists when the incident is beyond our and our IT provider's capacity, with the Management Sponsor's approval and, where relevant, the insurer's agreement.

17. Reporting to the authorities

The Incident Lead, with the Data Protection Officer and the Management Sponsor, decides which authorities to report to. Record each report, its reference number and the date and time it was made.

Authority	When to report	How
Information Commissioner (Office of the Information Commissioner, OIC)	Any security breach that affects or may affect personal data, and any contravention of the data protection standards, within 72 hours of becoming aware of it.	The Data Protection Officer submits the "Report a Data Breach" form on the OIC's official website. See section 13.
Jamaica Cyber Incident Response Team (JaCIRT), the Government of Jamaica's CIRT Division	Cyber incidents such as ransomware, intrusions, phishing campaigns and website compromise. Reporting helps the national team warn other organizations and may give us access to its help.	Use the incident report form on the JaCIRT website, cirt.gov.jm . Its form notes that it does not replace reporting obligations under the Data Protection Act.
Jamaica Constabulary Force (JCF)	Suspected crimes, including unauthorized access to computers or data, fraud, extortion and theft of devices. Offences such as these are covered by the Cybercrimes Act, 2015. Banks and insurers often ask for a police report.	Report to [nearest police station] and ask for the matter to be referred to the JCF's Communication Forensics and Cybercrime Division (CFCD). Get a reference number.
Sector regulator	If we are regulated, for example by the Bank of Jamaica or the Financial Services Commission, check our licence conditions and the regulator's rules for incident reporting.	[Regulator, contact and reporting requirements]

If we hold personal data about people in other countries, other countries' laws may also apply. Take legal advice.

18. Ransom and extortion demands

- Do not reply to, negotiate with or pay attackers without a decision from the Management Sponsor, taken with advice from our legal adviser and insurer.
- Paying does not guarantee that data will be restored or deleted, and may encourage further attacks.
- Report the demand to the police and to JaCIRT.
- Keep the ransom note and any messages from the attackers as evidence.

19. Testing the plan with a tabletop exercise

A tabletop exercise is a guided discussion in which the response team works through a realistic incident scenario, step by step, using this plan. It finds gaps in the plan, contact details and decision-making before a real incident does. Nothing is switched off and no live systems are touched.

- Run an exercise within [3] months of adopting this plan, then at least [once a year], and after any major change to our systems, people or this plan.
- Include everyone named in section 4, their deputies, and where possible our IT provider.
- Allow [2 to 3] hours. A facilitator presents the scenario in stages ("injects"), and the team decides what to do at each stage.
- Record the gaps found and agree actions with owners and due dates, as in a post-incident review.

Scenarios to choose from:

- ransomware found on a Friday evening before a public holiday, with the IT provider's main contact unreachable;
- a supplier "changes" its bank details by email and a large payment has already been sent;
- a laptop holding customer records is stolen from a staff member's car;
- a spreadsheet of customer details is emailed to the wrong recipient;
- a cyberattack during a hurricane-related power and internet outage;
- our IT provider tells us its own systems have been breached.

Questions the exercise should answer: Who is in charge? How do we talk if email is down? When did the 72-hour clock start, and who is drafting the report to the Information Commissioner? Who calls the bank and the insurer? What do we tell staff and customers, and when? Can we restore from backup, and how long would it take?

20. Training and awareness

- All staff are told how to recognize and report incidents when they join and in [annual] security awareness training.
- Members of the response team are briefed on this plan when they take on a role and take part in the tabletop exercise.
- Lessons from incidents and exercises are shared with staff, without naming individuals.

21. Plan maintenance and review

[Plan owner] reviews this plan every [12] months, after every Severity 1 or 2 incident, after each tabletop exercise, and when our systems, providers, staff or the law change. The emergency contact

sheet is checked every [6] months. Changes are approved by [Management Sponsor] and recorded in the document control table.

Appendix A: Emergency contact sheet

Keep this sheet up to date and keep printed copies off site. Check it every [6] months. Record the date checked: [date].

Role or organization	Name	Phone (office and mobile)	Email	After hours and notes
Incident Lead				
Incident Lead deputy				
Technical Lead				
Communications Lead				
Data Protection Officer or privacy lead				
Management Sponsor				
Log Keeper				
IT provider				
Internet service provider				
Cyber insurer (policy number)				
Bank fraud line				
Legal adviser				
Incident response specialist				
Office of the Information Commissioner	Report a Data Breach form on the official OIC website			

Role or organization	Name	Phone (office and mobile)	Email	After hours and notes
JaCIRT (CIRT Division)	Incident report form at cirt.gov.jm			
Police (nearest station)				
Sector regulator				
Key software or cloud provider				

Appendix B: Incident report form

Complete as much as you can. Do not delay reporting to fill in every box.

Question	Answer
Reported by (name, role, phone)	
Date and time of this report	
Date and time the problem was first noticed	
How was it noticed?	
What happened? Describe what you saw, in your own words	
Systems, devices, accounts or files affected	
Location or department	
Is it still happening?	
Could personal data be involved? What kind, and roughly how many people?	
What has been done so far, and by whom?	
Who else has been told?	
Evidence kept (emails, screenshots, photos)	
For the Incident Lead: incident reference number	
For the Incident Lead: severity level assigned	

Question	Answer
For the Data Protection Officer: personal data breach? Date and time we became aware	
For the Data Protection Officer: 72-hour deadline (date and time)	
Assigned to	

Appendix C: Incident log

Incident reference: [number]. Log Keeper: [name]. Record every action, decision, message and item of evidence as it happens. Use additional pages as needed.

Date and time	Who	Action, decision or observation	Decided or approved by	Evidence reference

Date and time	Who	Action, decision or observation	Decided or approved by	Evidence reference

Appendix D: First 72 hours timeline checklist

Time zero is when we become aware of the incident. Record it here: [date and time]. 72-hour deadline for the Information Commissioner, if personal data is affected: [date and time].

Hour 0 to 1

- ☐ Incident reported to the Incident Lead and an incident reference opened
- ☐ Incident log started, with the time we became aware
- ☐ Affected devices disconnected from the network (not switched off)
- ☐ Data Protection Officer told if personal data may be involved
- ☐ Severity level assigned and escalated as section 5 requires
- ☐ Out-of-band communication set up if email may be compromised
- ☐ Bank fraud line called if a fraudulent payment was made

Hours 1 to 4

- ☐ Response team assembled and tasks assigned
- ☐ IT provider engaged
- ☐ Insurer notified as the policy requires
- ☐ Containment steps under way (section 9)
- ☐ Logs exported and evidence preserved (section 15)
- ☐ Management Sponsor briefed and key decisions recorded
- ☐ Staff told what they need to know and what not to do

Hours 4 to 24

- ☐ Scope confirmed: systems, accounts, data and people affected
- ☐ Initial assessment of personal data affected and the risk to the people concerned
- ☐ Decision on outside specialists and legal advice
- ☐ Police report made where a crime is suspected, and reference number recorded
- ☐ Report to JaCIRT considered
- ☐ Holding statement and customer script prepared and approved
- ☐ Management Sponsor updated

Hours 24 to 48

- ☐ Containment confirmed, and eradication planned or under way
- ☐ Report to the Information Commissioner drafted by the Data Protection Officer
- ☐ Plan agreed for notifying affected people as required by the regulations

- ☐ Recovery priorities agreed with system owners
- ☐ Insurer and bank updated

Hours 48 to 72

- ☐ Report submitted to the Information Commissioner before the deadline, and its reference number recorded
- ☐ Follow-up reports scheduled if the report was made in phases
- ☐ Affected people notified, or notification under way, as required by the regulations
- ☐ Recovery under way and systems monitored
- ☐ Staff, customers and partners updated as needed
- ☐ Incident log complete and up to date

Appendix E: Post-incident review form

Item	Details
Incident reference and severity	
Dates: detected, contained, resolved, closed	
Review date and attendees	
Summary of what happened	
Root cause: how the attacker got in, or how the incident occurred	
How was it detected, and how long after it began?	
Impact: operations, finances, customers, staff and data	
Personal data affected (types and number of people)	
Reports made (Information Commissioner, JaCIRT, police, regulator) with dates and reference numbers	
Notifications made (affected people, insurer, bank, partners) with dates	
What worked well	
What did not work well	
Was this plan followed? Where was it unclear or missing something?	

Actions

Action	Owner	Due date	Status

Sign-off	Name	Signature	Date
Incident Lead			
Management Sponsor			