Data Breach Response Checklist

For Jamaican organizations. Prepared by Syxel Technologies Limited.

How to use this checklist

This checklist gives you a ready-to-use procedure for responding to a personal data breach. Delete this page before you adopt it.

- Replace everything in [square brackets] with your own details, and delete steps that do not apply to you.
- Name your breach lead (usually your Data Protection Officer or privacy lead) and a deputy in section 3, so someone can always act within the 72 hours, including on weekends and public holidays.
- Make sure everyone knows how to report a suspected breach (sections 3 and 4). Staff often see a breach first.
- Keep printed copies with the breach lead and deputy. If the breach is a cyberattack, email and file servers may not be available.
- Use the worksheet in Appendix A for every suspected breach, and record every breach in the register in Appendix C, including those you decide not to report.
- Practice using the checklist in a tabletop exercise, for example a customer list emailed to the wrong person.

This checklist is general guidance, not legal advice. It was prepared by Syxel Technologies Limited with the Jamaica Data Protection Act, 2020 in mind. For help with breach response planning or Data Protection Act compliance, contact sales@syxeltech.com.

[Organization] Personal Data Breach Response Checklist

Checklist owner	[Data Protection Officer or privacy lead]
Approved by	[Name, role]
Version	[1.0]
Effective date	[Date]
Next review	[Date, 12 months after the effective date]

1. When to use this checklist

Use this checklist whenever personal data held by [Organization], or by a provider on our behalf, may have been lost, stolen, destroyed, altered, disclosed or accessed without authorization. A breach does not have to involve hackers. Common examples include:

- an email or attachment containing personal data sent to the wrong person;
- a lost or stolen laptop, phone, USB drive or paper file;
- a staff email account taken over by an attacker;
- ransomware or other malware on systems that hold personal data;
- customer or employee records shared, viewed or downloaded by someone who should not have access;
- personal data published on a website or social media page by mistake;
- records destroyed or altered without authorization, or lost because a backup failed.

If the breach comes from a cyberattack, follow our [incident response plan] at the same time. This checklist covers the data protection steps; the incident response plan covers containment and recovery of the systems.

2. What the Data Protection Act requires

- 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 72 hours run from when we become aware of the breach. Weekends and public holidays count.
- The report must include prescribed details about the breach. The Information Commissioner's online breach report form allows a report to be made in phases, so report on time with what we

know and follow up as we learn more.

- People whose personal data is affected must be notified as required by the regulations.
- Breaching the standards, or failing to make a required report, can be an offense. A company convicted of an offense can be fined up to 4% of its annual gross worldwide turnover, and some offenses can lead to imprisonment.
- Registration requirements for data controllers have been phased in. Check the Office of the Information Commissioner's website for current registration requirements.

3. Who does what

Role	Held by	Responsibilities
Breach lead (Data Protection Officer or privacy lead)	[Name, role]. Deputy: [name, role]	Runs this checklist, assesses the risk to the people affected, makes the report to the Information Commissioner and oversees notifications.
Technical lead	[Name, role, or IT provider]	Finds out what data and systems are affected, contains the breach and preserves evidence.
Management	[Name, role]	Approves the report, notifications, spending and public statements.
Communications	[Name, role]	Drafts notifications, customer scripts and any public statement.
Everyone	All staff and contractors	Report a suspected breach immediately to [name, phone and email], and do not try to deal with it alone.

4. First hour

- [ ] Report the suspected breach to the breach lead [name, phone]. If you cannot reach them, call the deputy [name, phone].
- [ ] Record the date and time we became aware of the breach. This starts the 72-hour clock. Deadline: [date and time].
- [ ] Open a breach reference [format, e.g. DB-2026-001] and start a log of every action, decision and time.
- [ ] Stop the breach from continuing: for example, recall a misdirected email, lock a lost device remotely, reset a compromised password, or remove data published by mistake.
- [ ] If the breach comes from a cyberattack, disconnect affected devices from the network but do not switch them off, and start the incident response plan.
- [ ] Ask anyone who received data by mistake to delete it, not to share it, and to confirm this in writing.

- [ ] Preserve evidence: keep emails, logs, screenshots and photographs. Do not delete anything.
- [ ] Tell management.
- [ ] Keep knowledge of the breach to the people who need to know.

5. First 24 hours

- [ ] Complete the breach assessment worksheet (Appendix A) with the facts known so far.
- [ ] Identify the types of personal data involved, and whether any of it is sensitive personal data, such as health, biometric or criminal record information.
- [ ] Estimate how many people are affected, and in which groups: customers, employees, patients, students, members or others.
- [ ] Find out whether the data was encrypted or otherwise protected, and whether it has been recovered.
- [ ] Assess the likely consequences for the people affected, such as fraud, identity theft, financial loss, discrimination, damage to reputation or distress.
- [ ] If a service provider holds the data, get full written details from them and agree who will do what.
- [ ] Notify your insurer as your policy requires.
- [ ] If money may have been stolen or bank details exposed, contact the bank.
- [ ] Report to the police where a crime is suspected, such as theft or unauthorized access, and record the reference number.
- [ ] Consider reporting a cyberattack to the Jamaica Cyber Incident Response Team (JaCIRT) through its online form at cirt.gov.jm. This does not replace the report to the Information Commissioner.
- [ ] Take legal advice if the reporting position is unclear or the breach is serious.
- [ ] Brief management on the facts, the risk and the next steps.

6. By 72 hours: report to the Information Commissioner

- [ ] Decide whether the breach must be reported. If personal data is or may be affected, the starting point is that it must be. Record the decision and the reasons in the register (Appendix C).
- [ ] Draft the report using the facts in the breach assessment worksheet.
- [ ] Get the report approved by [management].
- [ ] Submit it through the "Report a Data Breach" form on the Office of the Information Commissioner's official website, before the 72-hour deadline. Check you are on the official site: the OIC has warned the public about a fraudulent website imitating it.
- [ ] If the facts are still incomplete, submit an initial report on time and say that follow-up information will be provided.

- [ ] Record the date and time of submission and the reference number the OIC gives.
- [ ] Diary dates for follow-up reports and send them as new facts emerge.

In general terms, the report describes:

- our organization, our contact person and Data Protection Officer, and any service provider involved;
- when the breach happened, when we became aware of it, how it was detected and its likely cause;
- whether the confidentiality, integrity or availability of personal data was affected;
- the types of personal data involved, 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 contain the breach, reduce the harm and prevent it happening again, including any report to the police;
- whether, how and when the people affected have been or will be notified.

7. Notifying affected people

People whose personal data is affected must be notified as required by the regulations. The breach lead decides, with management and legal advice where needed, who must be told, when and how.

- [ ] Confirm who must be notified, and check the current regulations and any guidance from the Information Commissioner.
- [ ] Draft the notification using the checklist in Appendix B.
- [ ] Choose a channel that reaches people reliably and securely. Do not use a compromised email account or system to send it.
- [ ] Get the notification approved by the breach lead and [management].
- [ ] Brief front-line staff with a short script and answers to likely questions before notifications go out.
- [ ] Send the notifications and record who was notified, when and how.
- [ ] Warn people to be suspicious of calls, messages or emails that claim to come from us about the breach and ask for passwords, PINs or payments.
- [ ] Track questions and complaints, and answer them consistently.

8. After the breach

- [ ] Confirm the breach is fully contained and the cause has been fixed.
- [ ] Send any follow-up or final report to the Information Commissioner.
- [ ] Complete the entry in the breach register (Appendix C).

- [ ] Hold a review within [10] working days: what happened, why, how we responded and what to change.
- [ ] Agree improvement actions with owners and due dates, such as encryption, multi-factor authentication, access reviews, training or changes to a process.
- [ ] Update policies, procedures, privacy notices and contracts with service providers where needed.
- [ ] Brief staff on the lessons learned, without naming individuals.
- [ ] Review this checklist and update it.

9. Records to keep

Keep these records for [period, e.g. at least six years] in a location with restricted access:

- the breach log and completed breach assessment worksheet;
- the report to the Information Commissioner, any follow-up reports and the OIC reference number;
- copies of notifications sent, with the list of people notified and dates;
- reports to the police, JaCIRT, the insurer, the bank and any regulator, with reference numbers;
- the review findings and the action plan;
- the breach register entry, including the reasons for any decision not to report or not to notify.

Appendix A: Breach assessment worksheet

Complete this worksheet for every suspected breach and update it as facts emerge. It feeds the report to the Information Commissioner and the decision on notifying people.

Question	Answer
Breach reference	
Date and time we became aware	
72-hour deadline (date and time)	
Date and time the breach happened, if known	
How was it detected, and by whom?	
What happened? Describe the facts	
Likely cause (for example human error, theft, cyberattack, system failure)	
Was confidentiality, integrity or availability affected?	
Systems, files or records involved	
Types of personal data involved	
Is any of it sensitive personal data? Which types?	
Approximate number of people affected	
Categories of people (customers, employees, patients, students, children, others)	
Where are the people affected located (Jamaica, elsewhere)?	

Question	Answer
Was the data encrypted or otherwise protected?	
Has the data been recovered or deleted by the recipient?	
Who has, or may have, the data?	
Service provider involved (name, contact)	
Likely consequences for the people affected	
Risk to the people affected: Low, Medium or High, and why	
Steps taken to contain the breach and reduce the harm	
Report to the Information Commissioner: yes or no, and reasons	
Notify affected people: yes or no, and reasons	
Other reports: police, JaCIRT, insurer, bank, regulator (dates and references)	
Completed by and date	
Reviewed by (breach lead) and date	

Appendix B: Draft notification checklist

Use this checklist to draft and check a notification to the people whose personal data is affected.

Contents

- [ ] A plain-language description of what happened and when
- [ ] The types of their personal data involved
- [ ] The likely consequences for them
- [ ] What we have done, and are doing, to deal with the breach and reduce the harm
- [ ] What they can do to protect themselves, such as changing passwords, watching bank and card statements, and being alert to suspicious calls and messages
- [ ] A clear statement that we will never ask for passwords, PINs or payment details in connection with the breach
- [ ] Who to contact with questions, including our Data Protection Officer's contact details
- [ ] An apology, where appropriate

Checks before sending

- [ ] The facts match those in the report to the Information Commissioner
- [ ] It is written in plain language, without technical or legal jargon
- [ ] It does not include more personal data than needed, or details that would help an attacker
- [ ] Approved by the breach lead and [management], with legal advice where needed
- [ ] Front-line staff have been briefed and have a script
- [ ] The sending channel is secure and not the one that was compromised
- [ ] A record will be kept of who was notified, when and how

Appendix C: Breach register

Record every personal data breach and suspected breach here, including those not reported to the Information Commissioner, with the reasons.

Reference	Date aware	What happened	Data and number of people	Risk	OIC report (date, reference) or reason not reported	People notified (date, how)	Actions and date closed