Data Breach Response
Your First 72 Hours

A step-by-step guide for Jamaican businesses

GHS Data Security Limited

admin@ghsdatasecurity.com

Data Breach Response Flowchart

PHASE 1: CONTAIN AND ASSESS (Hour 0 to 4)

Action	Details	Responsible
Isolate affected systems	Disconnect compromised devices. Change passwords. Disable breached accounts.	IT / Security Lead
Preserve evidence	Do NOT delete logs, emails, or files. Screenshot error messages. Record timestamps.	IT / Security Lead
Initial assessment	What data was affected? How many people? Is data encrypted? Was it accessed, stolen, or just exposed?	IT / Security Lead
Activate response team	Notify DPO, senior management, legal counsel, and IT security.	Incident Lead
Document everything	Start an Incident Log. Record all actions, decisions, and timestamps from this point forward.	All

PHASE 2: INVESTIGATE AND ESCALATE (Hour 4 to 24)

Action	Details	Responsible
Full investigation	Determine root cause. Identify all affected data and systems. Assess the scope.	IT / CISO
Risk assessment	Is this a notifiable breach? Does it pose a risk to the rights and freedoms of individuals?	DPO / Legal
Prepare OIC notification	Draft the notification report including: description of breach, categories of data, number of individuals, lik	DPO
Prepare communications	Draft internal briefing for staff. Draft external communication for affected individuals (if required).	Comms / DPO
Brief senior management	Present findings, risk assessment, and recommended actions to leadership.	Incident Lead

PHASE 3: NOTIFY AND REMEDIATE (Hour 24 to 72)

Action	Details	Responsible
Submit OIC notification	File breach notification with the Office of the Information Commissioner within 72 hours of discovery.	DPO
Notify affected individuals	If high risk: notify individuals directly. Explain what happened, what data was involved, and what they sh	Comms / DPO
Implement remediation	Patch vulnerabilities. Update access controls. Strengthen security measures.	IT / CISO
Conduct post-incident review	What went wrong? What worked? Update your Breach Response Plan based on lessons learned.	All
Update documentation	Finalise incident log. File all evidence. Update ROPA if processing activities have changed.	DPO

Key Contacts Template

Fill in and keep this template accessible to your incident response team.

Role	Name	Phone	Email
Incident Lead			
Data Protection Officer			
IT / Security Lead			
Legal Counsel			
Senior Management Contact			
OIC Contact	Office of the Information Commissioner	(876) 920-4027	info@oic.gov.jm
GHS Data Security (External)	GHS Data Security Limited	(876) 555-0199	admin@ghsdatasecurity.com

---