procedure for Handling data Breaches

Purpose	The purpose of the procedure is to outline the rigorous steps that xy innovate have taken and that I have drafted to manage data breached effectively. In my breakdown I have ensured that I have integrated a level of regulatory compliance for example GDPR article 33 whole safeguarding sensitive customer information include PII and financial details. The procedure has a clear alignment with the ISO 27001 framework to ensure that data breaches are effectively managed, and the impact is mitigated to cause the least amount of damage to the organization and individuals involved.
Scope	This procedure for handling data breaches would apply to all employees and individuals, contractors, external 3rd parties who are involved in analysing, maintaining or reviewing key customer financial information including the digital wallet application and the HR management systems alongside the data servers in our physical locations. This involves reviewing internal and external processes that would result in a data breach, so this is a comprehensive approach to security management.
Process Steps Detailed breakdown below	1) Incident detection 2) Immediate notification of the issue 3) Conduct the initial assessment 4) Deploy the relevant containment measures 5) Perform a root cause analysis 6) Deploy a data breach notification 7) Perform the remediation and recovery plan 8) Conduct a post breach review

1) Incident Detection- This is the first step in the procedure that I have drafted to manage a data breach. Data breaches as mentioned previously can be monitored and detected through system monitoring and monitoring user logs and utilising automated tools and systems such as SEIM platforms which proactively monitor the system and create alters for anomalies in the system such as unauthorized credential access and unique data usage/transfer between individuals. The individuals responsible for this would be the IT department and the digital wallet services team s they would ensure that the tools are being utilised correctly to get to the desired outcomes of being able to correctly identify any threats in the system.

2) Immediate notification of the issue – Once this breach has been identified we will now ensure that it is reported as soon as possible to the relevant incident response team by a secure procedure called the incident reporting system which

would have a layer of encrypted security so this cannot be accessed or breached. Employees will be responsible in identifying threats if they are clear and apparent and the relevant security training will be provided to them to be able to identify threats in the system and their devices and report any suspicious activities and to escalate appropriately. This fast-paced response to a threat directly aligns with the ISO / IEC 27035's (Rapid7, 2025). Focus on early detection and response.

3) This is the initial assessment process, the Internal Audit Supervisor Tom Knowles alongside the digital wallet services and IT team will create a joint taskforce to conduct an initial assessment to determine the impact and scope of the recent breach and this would include understanding the type of data that has been corrupted what has been affected or changed such as personally identifiable information. This stage will include identifying the identity of the threat actor to block access or any ways this individual could gain access to our organisation.

4) The next step in my procedure is to deploy containment measures around the organisation order to not be exposed to any further damage the IT security team would isolate the effected system and to revoke credentials that may have been used in the breach and now classified as compromised. This step will include deploying a failover system or utilising backup servers to ensure the business maintains its productivity and daily operations. An example of this in action is that if the breach involved the digital oceans systems and the data stored in it a system would immediately be put in place to secure the cloud storage system.

5) The next step would be to conduct a root cause analysis. To minimise any further damage an investigation would be launched into understanding where the breach originated from and how it was able to break into our systems. We would then examine all the vulnerabilities in our system and where the cause of the issue originated from. This may be outdated access controls or outdated security patches alongside simple employee errors. The result of this investigation guides our implementation of placing processes in place to ensure increased stability and security.

6) The Notification of the data breach occurrence. In most instances GDPR regulations ensures that the individuals responsible for mainting security i.e. a ciso would need to report and inform the relevant individuals of a security breach within the 72-hour notice period. This is something I am focusing heavily on as transparency and accountability is a huge factor in overall organizational success and to reduce the impact that the data breach may have on the company.

7) Perform the remediation and recovery plan – In this section of the policy I have purposefully placed this at this current point because will all the additional steps in place we should have enough information gathered to implement the recovery plan. The IT and digital wallet service team will ensure that the systems that have been affected are restored back to normal using the backup stores that we have. The integrity of the system will also be monitored to ensure that there are no remaining vulnerabilities. This would align with the ISO/IEC 27031's (ISO/IEC, 2025). Emphasis on business continuity readiness.

8) Post breach Review – This step is crucial as it allows us to review the controls we have implemented and see the effectiveness of this over a period post breach. We would analyse the incident; document the new information we have learnt and identify where would improve. Once this has been done, we would update the policies and procedures based on the new findings to improve he security of our information security management system.

Rapid7, 2025. Introduction to ISO/IEC 27035 - Planning for and Detection of Incidents. *Rapid7 Blog*. Available at: Introduction to ISO/IEC 27035 - Planning for and Detection of Incidents | Rapid7 Blog [Accessed 2 January 2025].

ISO/IEC, 2025. ISO/IEC 27031 ICT for Business Continuity. *ISO/IEC*. Available at: Business & ICT Continuity (ISO 22301 & ISO 27031) | Business Beam [Accessed 2 January 2025].