Cognitive Automation Labs: Data Breach Procedure

Data Breach Procedure

1. Identify and Isolate: Upon discovering a potential data breach or suspecting unauthorized access to sensitive data, take immediate action to identify and isolate the affected systems or data. This may involve disconnecting affected devices from the network or disabling compromised user accounts.
2. Notify Relevant Parties: Notify the appropriate individuals or departments, including IT security personnel, data protection officers, and senior management. Provide them with the necessary details regarding the suspected data breach, including the date, time, and potential scope of the incident.
3. Preserve Evidence: Preserve any evidence related to the data breach. Avoid altering or deleting any files or logs that could be crucial for forensic investigation or legal purposes. Document the steps taken, including any actions performed to mitigate the breach.
4. Engage IT Security and Forensics Experts: Engage the services of IT security and forensics experts to investigate the breach further. They will assess the extent of the breach, identify the vulnerabilities or entry points, and provide recommendations for remediation.
5. Assess the Impact: Conduct a thorough assessment to determine the impact of the data breach, including the potential compromise of sensitive data, the number of affected individuals or accounts, and any regulatory or legal obligations that may arise.
6. Mitigate and Remediate: Take immediate steps to mitigate the breach and prevent any further unauthorized access. This may involve patching vulnerabilities, enhancing security controls, or implementing additional safeguards to protect against similar incidents in the future.
7. Evaluate and Learn: Conduct a post-incident analysis to identify the root causes of the breach and evaluate the effectiveness of existing security measures and protocols. Implement any necessary improvements or changes to prevent future breaches.
8. Update Authorities and Regulatory Bodies: If required by law or regulations, report the data breach to the appropriate authorities or regulatory bodies within the specified timeframe. Provide them with the necessary information and cooperate fully during any subsequent investigations or audits.
9. Communicate Internally and Externally: Keep all relevant stakeholders informed throughout the incident response process. This includes employees, clients, partners, and any other parties affected or involved. Provide regular updates regarding the breach, the actions being taken, and any changes in data protection measures.

Prepared by:	Joanne Parsons – Head of Business Administration
Approved by:	Jonathan Parsons – Co-Founder & CEO
Last Modified:	11/10/2022