Alcedo, Luis Carmelo C. **Dishoco, Eliah Kim** **Papillero, Christine Mae D.** **Renido, Kyron** **Suarez, Son Zoe M.**	**Apr 22, 2024** **Ms. Jasmin Gas** **CS32S2**

1. Purpose

The purpose of this policy is to provide a structured and effective response to data breaches, specifically unauthorized access, aimed at minimizing their impact, protecting customer information, ensuring compliance with all relevant regulations, and maintaining the integrity and reputation of Kyronics Techno Corp.

2. Scope

This policy applies to all employees, contractors, and third-party service providers of Kyronics Techno Corp. It encompasses all forms of data handled by the company, both digital and physical, across all departments and platforms where data is stored or processed.

3. Policy Overview

Detection and Reporting

The objective of this section of our policy is to quickly identify and report unauthorized data access to appropriate internal authorities. To achieve this, we will implement automated systems to monitor for unusual access patterns and potential security breaches. Additionally, we will train employees to recognize and immediately report any security incidents, ensuring a rapid and efficient response to potential threats.

Assessment

The objective of this section is to promptly assess the severity and scope of any data breach. To facilitate this, we will form a dedicated response team tasked with determining the data affected, identifying the cause of the breach, and evaluating the potential impact on both the company and affected individuals. This structured approach ensures a thorough and swift assessment, enabling effective management and mitigation of any data breach incidents.

Compliance

This section is to ensure that all actions taken in response to a data breach comply with legal and regulatory requirements. To achieve this, we will regularly review and update our compliance protocols to adhere to laws such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and other relevant regulations that pertain to the locations and sectors in which our company operates. This process guarantees that our data breach response is not only effective but also legally compliant.

Alignment to Industry Standards

To align the company's breach response with best practices and standards within the industry. To accomplish this, we will adopt frameworks and guidelines from recognized standards such as ISO/IEC 27001 for information security management and NIST guidelines for cybersecurity. This adherence to established protocols ensures that our response to data breaches is consistent with industry-leading practices, enhancing our overall security posture and credibility.

Containment and Eradication

The breach promptly and eradicate the source of the breach to prevent further unauthorized access or damage. Our procedures to meet this objective include isolating compromised systems, removing unauthorized access points, and securing network vulnerabilities. These steps are crucial for halting the spread of the breach and ensuring that the integrity of our systems is restored, safeguarding against future security threats.

Notification

Notify all impacted parties, including regulatory authorities and affected individuals, in a timely and legally compliant manner. To fulfill this objective, we will follow predefined communication plans that specify the timing, method, and content of notifications, as dictated by legal requirements and company standards. This structured approach ensures that all communications are managed effectively, maintaining transparency and adhering to regulatory obligations during a data breach response.

Recovery

This is to restore affected services and data, and to reinforce systems against future breaches. To achieve this, we will implement recovery plans that involve restoring data from backups, repairing damaged systems, and hardening defenses against future attacks. These procedures are critical for ensuring that operational continuity is quickly reestablished while also enhancing the security measures to prevent recurrence of similar incidents.

Post-Incident Analysis

Thoroughly analyze the breach and integrate the lessons learned into future security practices. To achieve this, we will conduct a comprehensive investigation to identify the root cause of the breach, document our findings, and develop recommendations to strengthen our policies and systems. These steps are essential for preventing similar incidents in the future and enhancing our overall security framework. This proactive approach not only mitigates immediate risks but also contributes to the long-term resilience of our organization.

Review and Updates

This is to continuously improve the breach response policy and practices based on new information, evolving threats, and regulatory changes. To meet this objective, we will regularly review and update the policy, at least annually or following significant incidents. This process will allow us to incorporate new insights, adapt to changing security landscapes, and ensure compliance with updated regulations. This proactive approach ensures that our policies remain effective and relevant, thereby strengthening our preparedness and response capabilities against potential data breaches.