Measures to Data Breach （Cyber Incident Response Plan ）

[Establishment of Policies and Procedures]
We have established internal management rules that set forth policies, procedures, organizational structures, and other matters relating to cybersecurity incidents.

[Organizational Framework]
We have established the Information Crisis Management Department as the organization responsible for responding to security incidents and large-scale system outages. Within this department, a CSIRT has been established as a dedicated incident response team. In the event of an incident, the CSIRT works in coordination with relevant departments to take initial response measures, identify the scope of impact, and prevent further damage. In addition, information is consolidated and reported to the Security Committee, which comprises Directors, the CRO, CIO, CISO, and other relevant members. The Committee is responsible for deliberating on and determining response policies.

[Prevention/Preparedness]

(Identification of Critical Assets and Risk Assessment)
We identify and review the status of our cybersecurity infrastructure and security measures, while also assessing threats and risks to our information assets.

(Scenario Analysis)
Based on the results of risk assessments, we conduct scenario analyses and regularly carries out simulation exercises involving all relevant stakeholders in accordance with the identified scenarios.

(Vulnerability Analysis)
We monitor newly identified vulnerabilities, developments in emerging technologies, intrusion activities, and related trends to determine whether there have been any changes in cybersecurity risks, and implements necessary measures as appropriate.

(Analysis of Logs and Alerts)
We analyze logs and alerts from security systems to detect signs of anomalous activity and determine whether any security breaches have occurred.

(Incident Reporting and Escalation)
We have established an incident response flow that includes a designated point of contact for reporting security incidents, reporting and communication procedures, and escalation routes based on the severity of the incident.

(Security Education and Awareness)
We provide all employees with security training and incident response exercises, including phishing simulations. We also regularly share security-related information, examples of security incidents, and alerts and reminders to raise awareness.

Measures to Data Breach（Cyber Incident Response Plan ）

[**Incident Response**]

(**Incident Assessment**)

We receive signs of security anomalies, such as alerts detected by various security systems and reports from users, as security events and determine whether they constitute security incidents. We identify the impact on business operations and the scope of impact, assess their priority, and determine whether a response is required. Significant incidents are also reported to the Security Committee and the Risk Management Committee.

(**Root Cause Analysis**)

We analyze logs and other relevant information to identify the attack vector, vulnerabilities, attack methods, and root cause of the incident.

(**Containment and Eradication**)

We promptly implement measures to prevent further damage, such as disabling accounts, isolating or blocking network connections, and disconnecting infected devices. We also remove or remediate malware, unauthorized configurations, unauthorized accounts, vulnerabilities, and other causes to prevent recurrence or reintrusion. Through these measures, we seek to minimize the impact of the incident.

(**Recovery**)

We take measures to ensure business continuity, such as implementing alternative operations and resuming services. After eliminating the cause of the incident and confirming system security, we restore systems and business-related data.

(**Reporting and Notification**)

We compile information on the nature of the cyberattack, the scope of its impact, the response process from incident detection through recovery, and the results of the response. We report this information to relevant internal stakeholders, including senior management, and, where necessary, provide reports and notifications to customers, business partners, and other relevant parties.

[**Post-Incident/Improvement**]

(**Post-Incident Review**)

We evaluate the causes and impact of the incident, the response taken, and the recovery results, and identify issues and lessons learned.

(**Preventive and Improvement Measures**)

Based on the causes of the incident and the results of the post-incident review, we implement measures to prevent recurrence, such as strengthening security controls, improving processes, and adding monitoring rules. As necessary, we also review and revise relevant policies, organizational structures, and plans. We further incorporate lessons learned and incident examples into our training and exercises and update them accordingly to help prevent recurrence.