Information Security and Privacy Policy

1. General Provisions

1.1. Purpose

This policy is intended to protect the important information assets of LG CNS Co., Ltd. (hereinafter referred to as "the Company") and clients who use the Company's services. It complies with relevant laws and regulations and establishes the necessary measures for information security and personal information protection to protect important information from risks such as misuse, destruction, unauthorized alteration, and data breach.

1.2. Scope and Application

1.2.1 This policy applies to all employees, third-party contractors and service providers working at the Company.

1.2.2 This policy applies to all assets owned by the company, including tangible and intangible assets, as well as assets derived from human resources such as personal information of employees, clients, and business partners, and all related activities.

2. Information Security Management Policy

2.1. Information Security Policy Management

We establish regulations that clearly state the management's commitment and management direction for information security, as well as detailed rules for each area of information security, and continuously review and improve them to ensure compliance with relevant laws, regulations, and international standards.

2.2 Information Security Organization

2.2.1 In order to systematically implement information security management activities, an organization shall be established consisting of a chief information security officer and chief privacy officer who oversee information security and personal information protection company-wide, a department in charge of information security and personal information protection, relevant departments, and responsible personnel.

2.2.2 In order to smoothly perform tasks related to information security consultation, coordination, planning, and performance, an Information Protection Committee and an Information Security Council shall be established and operated.

2.3 Identification and Security Management of Information Assets

2.3.1 We identify, classify, and rate all information assets (servers, PCs, networks, documents, etc). We identify security threats through risk assessment and apply protective measures.

2.3.2 Security requirements shall be reflected throughout the entire process of information system development, operation, and disposal, and protective measures such as access control, encryption, and backup shall be implemented.

2.4 Human Resource/Physical Security

2.4.1 We conduct security training, confidentiality agreements, and access control for employees and external parties, and implement measures to prevent information leakage.

2.4.2 We establish security areas and apply physical protection measures such as access control and installation of CCTV.

2.5. Cloud Security

2.5.1 When introducing cloud services, the Company shall select service types based on physical location, data classification, management and operational levels, and shall conclude service agreements that reflect security requirements.

2.5.2 The Cloud Standard Security Architecture must be followed, and systematic security management measures must be established from the creation and change management of new virtual assets to the termination of operations.

2.6 Information Security Inspection and Audit

2.6.1 The Company shall conduct regular inspections to confirm that there are no violations of domestic and international information security and personal information protection laws and regulations, as well as the Company's policies, and shall make improvements as necessary.

2.6.2 Information security・Personal information protection department shall confirm compliance with policies through regular and irregular inspections and audits and shall take necessary measures when necessary.

2.7 Information Security Training

2.7.1 The information security department shall operate information security and personal information protection training programs to raise awareness of information security among employees and external parties.

2.7.2 We regularly conduct information security and personal information protection training, by establishing training plans that include training methods, targets, and content, analyzing the results of the training, and making improvements.

3. Privacy Policy

3.1 Protection of personal information throughout the company

3.1.1 The following items regarding personal information processing standards and protection of information subject rights shall be observed.

1) Establishment and implementation of internal management plans for personal information
2) Personal information handling standards
3) Guarantee of rights of information subjects
4) Application of measures to ensure the security of personal information
5) Protection of anonymous and pseudonymous information
6) Installation and operation of CCTV
7) Notification and reporting of personal information leaks

3.1.2 The department in charge of personal information protection shall regularly review and improve matters stipulated in personal information protection laws and regulations.

3.2 Basic Principles of Personal Information Protection

1) Refrain from indiscriminate collection of personal information
2) Distinction between required and optional information when collecting personal information
3) Sensitive information such as national personal identification number and other unique identifiers, as well as religious and health information, shall not be processed in principle
4) When entrusting personal information for promotional or sales purposes, notify customers and manage it thoroughly.
5) Personal information shall be handled using secure methods such as data encryption
6) Compliance with retention periods stipulated by laws and regulations when storing personal information
7) Destruction of personal information so that it cannot be identified when the information is unnecessary
8) Signs must be installed on CCTV for notification
9) Be sure to have guidelines and documents related to personal information protection
10) Guarantee of rights of information subjects and preparation measurements for personal information leakage, collective dispute mediation, and class action lawsuits

4. Security Incident Response

4.1 Security Incident Response System and Post-Incident Management

4.1.1 We establish security incident response procedures and respond to incidents in accordance with the procedures when security incidents occur.

4.1.2 In order to respond to security incidents in a systematic and efficient manner, we will conduct regular incident response trainings and education to continuously improve our response system.

5. Disaster recovery

5.1 System Establishment and Follow-up Management

5.1.1 For rapid recovery, a disaster recovery system shall be established, including a disaster recovery team consisting of relevant departments and information security departments, and responsibilities and roles shall be defined.

5.1.2 We define recovery priorities and recovery objectives through business impact analysis and establish a system capable of recovering within an appropriate time frame.

5.1.3 We conduct regular trainings to ensure that strategies and measures in accordance with the disaster recovery plan can achieve recovery objectives.