

Information Security Policy and Privacy Policy

This policy aims to establish fundamental guidelines to protect the company's personal information from misuse, damage, alteration, and leakage by authorized and unauthorized individuals, in accordance with the basic principles declared in the information security policy to maintain business continuity and competitiveness. LG Display's privacy policy applies to all domestic and overseas subsidiaries, joint ventures, suppliers, and personal information processing contractors and subcontractors.

▪ Information Security Policy

Category	Details
Information Security Policy Direction	<p>LG Display strengthens employees' awareness of information security, prevents data leakage, and applies information security across all business operations to ensure service availability.</p> <ul style="list-style-type: none"> • Information security training is conducted to enhance employees' awareness and responsibility regarding information security. • Unauthorized access and alteration are prevented to ensure the integrity of information. • Regular internal audits are conducted to verify that information security-related operational procedures are properly implemented. • The company manages its major systems to maintain availability at or above a certain level.
Continuous Improvement of the Information Security Framework	<p>LG Display systematically operates its information security policies and continuously improves its security framework to maintain an international level of security.</p> <ul style="list-style-type: none"> • A dedicated information security organization is operated to oversee and implement information security policies. • Regular internal audits and information security governance assessments are conducted to continuously ensure that operational levels comply with established standards. • The company maintains international information security certifications such as ISO 27001 and TISAX. • LG Display strengthens its overall information security capabilities by establishing proactive detection and response systems.
Ensuring Data Integrity and Protection	<p>LG Display securely protects and stably operates its critical information and data assets.</p> <ul style="list-style-type: none"> • The company protects its business information from unauthorized access, modification, or destruction. • To ensure the availability of critical information, LG Display regularly verifies data accuracy and system integrity. • The company continuously optimizes its information management and operational processes by adopting external information security solutions.
Monitoring and Response to Information Security Threats	<p>LG Display conducts continuous monitoring and response activities to prevent information security incidents and strengthen response capabilities.</p> <ul style="list-style-type: none"> • Regular security training and simulation exercises are conducted to enhance response capabilities. • The company strengthens its security response capabilities by sharing information on security threats in cooperation with the Korea Internet & Security Agency (KISA) and relevant organizations.
Employee Information Security Management and Awareness Enhancement	<p>LG Display promotes activities to establish an information security culture and strengthen employees' sense of responsibility.</p> <ul style="list-style-type: none"> • Information security training is conducted to enhance employees' awareness and accountability regarding information security. • The company regularly conducts awareness campaigns and related activities to foster a company-wide information security culture.
Establishment of Supply Chain Information Security Requirements	<p>LG Display manages security requirements to minimize information security risks across the entire supply chain.</p> <ul style="list-style-type: none"> • The company reduces supply chain-based information security risks by requiring partners and third parties to comply with its information security policies and related operational standards.

▪ Privacy Policy

Category	Details
Privacy policy	LG Display has established and implemented a privacy protection policy that includes technical, physical, and administrative measures. Technical protective measures include network security and malware prevention. Physical protective measures involve access controls to data centers and document storage rooms. For administrative measures, LG Display enforces internal privacy protection guidelines and ensures that all employees are aware of the importance of privacy protection and apply it to their work through the distribution of a 'Privacy Protection Guide' and regular training.
Designation of privacy protection manager	LG Display has designated a Chief Privacy Officer (CPO) to protect the company's and stakeholders' information. The CPO oversees the information security and privacy protection functions, and an organization dedicated to these areas operates under their authority. The Chief Privacy Officer is responsible for overseeing personal information processing activities and managing privacy protection efforts.
Privacy protection policy system included in group-level risk/compliance Management	Privacy protection, which is included in the company's compliance management areas, is one of the major risk areas addressed through annual compliance checks and compliance training. Additionally, through the legal system, we review personal information handling practices at the contract review stage with domestic and international subsidiaries, joint ventures, suppliers, and contractors. At the time of contract signing, we collect and manage Personal Information Processing Subcontractor Commitment forms.
Disciplinary actions for privacy protection	If any violations related to privacy protection are discovered, penalties are imposed on the violators in accordance with the zero-tolerance principle.
Auditing of compliance the privacy policy	LG Display conducts an annual compliance check to ensure adherence to its privacy protection policies. Additionally, to prevent the misuse or leakage of personal information according to the policies, the company conducts internal audits at least once a year and third-party audits at least once every two years.