KERING

KERING GLOBAL INFORMATION SECURITY POLICY 2025

40, rue de Sèvres
Paris 7e - France
kering.com

Contents

1. Document management

Version	Date	Redactor	Company / entity	Changes and motivation	Section
V0.01	15/05/2021	Anonymized	Kering technology	First version	all
V2021	29/09/2021	Anonymized	Kering technology	Validation & publication	all
V2023	15/05/2023	Anonymized	Kering technology	Revision of document management	1
V2024	08/04/2024	Anonymized	Kering technology	Change on compliance / Status update	all
V2025	02/07/2025	Anonymized	Kering Technology & Digital (KTD)	Refresh	all

2. Introduction

Kering is a global, family-led luxury group, home to people whose passion and expertise nurture creative Houses across couture and ready-to-wear, leather goods, jewelry, eyewear and beauty which spread over a large number of geographical locations. A current list of Kering Brands is available on https://www.kering.com.

Kering considers Information to be one of its most valuable assets. It is a key factor of the Group's growth and customers' trust.

As such, Information (in particular as collected in numerical form and processed in Kering Information System) together with the Information System that is used to process it and provides Kering Group with services that are vital for its activities, need to be adequately protected against increasing Threats both internal and external to Kering such as, without limitation, logical intrusions, information theft, sabotage, Social Engineering, cyber terrorism.

Protecting Information means ensuring the confidentiality, integrity and availability of the Information.

If Information is lost, stolen, inappropriately disclosed, destroyed, modified, serious consequences may result for Kering such as:

- Loss of customers' trust (in particular following a personal data breach or the unavailability of sales and/or payment services.
- Loss of competitive advantage (e.g. in the event of theft and disclosure of know-how and trade secret);
- Loss of revenue (in case of unavailability of key components generating value (e-commerce websites, payment services…).

Adding to the challenge of securing Information, which has become paramount, is the increasing push for compliance with legal and regulatory requirements for privacy and security of the Information.

It is Kering responsibility to ensure the confidentiality, integrity and availability of the Information that is processed on or transits its Information System while at the same time complying with all applicable statutory and legal requirements.

The **Global Information Security Policy** ("**GISP**") set out below is an important milestone towards an effective Information Security management within Kering Group and is of critical importance to all Kering Group stakeholders – employees, management and shareholders – as well as to its customers and suppliers.

3. Purpose of Kering Global Information Security Policy

Kering's Information System and the Information it holds must be protected in a pragmatic, evolving and flexible way through a robust Information Security Program. This Information Security Program is described in this GISP.

This GISP provides global security principles to enhance information security management within the Group and reduce the risks linked to the Information System.

The main purpose of this GISP is to define Kering's main orientations regarding Information Security Management. Its objectives are to:

- Protect the Information and the Information Systems,
- Protect Kering Users,
- Mitigate the risks associated to the theft, loss, misuse, damage or abuse of the Information Systems,
- Maintain customer trust and confidence,

- Protect Kering image and reputation.

More precisely, this GISP:

- Reflects and formalizes Kering Group Top Management's strategy and objectives for securing Information.
- Identifies the essential roles and responsibilities and governance in order to achieve these security objectives.
- Describes the key features of Kering Group Information Security framework.

A secondary very relevant purpose of this GISP is to ensure that all Kering Users understand their responsibilities for protecting the confidentiality and integrity of the Information they handle.

The principles provided in this GISP will be implemented by functional policies (and support with procedures and guidelines) listed in Section 6.6.

4. Scope of Kering Global Information Security Policy

This Global Information Security Policy applies to all Kering Users who access the Information that is processed on or transits the Information Systems regardless of their location (Europe, Middle-East, Africa, Americas or Asia) or their place of work.

It also applies to the use of all Information Systems, whether used for business purposes or private purposes and to any message or content sent, received, stored by or on any Information System.

This GISP also applies to Kering Service Providers who are given access to the Data and the Information Systems.

5. Legal, Regulatory and Normative Compliance

Kering SA and its Affiliates are subject to a broad set of legal, regulatory, contractual, and normative obligations, and must ensure that their activities are conducted in compliance with national and international laws, as well as with applicable industry standards and best practices.

5.1. Regulatory and Legal Compliance

As legal entities, Kering and its Affiliates are required to

- Ensure their operations are fully compliant with local and international legislation, including but not limited to areas such as data protection, intellectual property, and cybersecurity.
- Be capable of providing legal evidence related to IT processing activities, particularly in the event of fraudulent operations or misappropriation of funds.

Kering Users must comply with the legislation applicable in any country where Kering operates. This includes adherence to:

Global Data Protection Regulations, such as but not limited to:

- EU General Data Protection Regulation (GDPR)
- China Cybersecurity Law (CSL) and Personal Information Protection Law (PIPL)
- Asia & Pacific countries regulations (Korea, Japan, …etc)
- United States of America specific regulations, Canada, Brazil…etc

Contractual Obligations, including:

- Customer contracts that define specific security requirements
- Supplier agreements with minimum security conditions
- Cyber insurance policies requiring the implementation of risk-mitigation controls
-

5.2. Normative and Industry Standards Alignment

Kering's information security policies and controls are aligned with globally recognized **standards and frameworks**, forming an integrated and coherent compliance structure:

Management System Standards :

- **ISO/IEC 27001:2022 –** Information Security Management System (ISMS) requirements
- **ISO/IEC 27002:2022** – Guidelines for implementing information security controls

Industry Security Standards :

- **Payment Card Industry Data Security Standard (PCI DSS) v4.0** – Technical requirements for handling cardholder data
- **SWIFT Customer Security Programme (CSP)** – Mandatory controls for financial institutions connected to the SWIFT network

Risk Management Frameworks :

- **NIST Cybersecurity Framework (CSF) 2.0** – Risk-based approach to cybersecurity governance and controls

6. Governance

6.1. Roles and Responsibilities

The roles and responsibilities under the Information Security Program are described in this section.

The Chief Information Security Officer — CISO (and the Cybersecurity Team)

The CISO is responsible for developing, managing, maintaining and implementing this GISP and its related Operational Policies – specific policies, procedures and technical security measures – of the Group. The CISO is also responsible for establishing and maintaining an Information Security awareness program in order to ensure that Kering Users awareness is maintained and updated as necessary. Finally, the CISO is responsible for information security crisis and incident management and the integration of security requirements into project management.

The Internal Audit Department

The Internal Audit Department supports Kering Management in the assessment and management of business risks, including Information Security risks and ensure controls are in place and effective in addressing those risks. As part of its global mandate, the Internal Audit Department controls and assesses the proper implementation of the security measures described in this Global Information Security Policy and its Operational Policies.

The Security Department

The Security Department is responsible for the physical and environmental security of Kering SA and its Affiliates' sites, offices and stores.

The Legal Department

The Legal Department is responsible for identifying, analyzing and implementing the legislative and regulatory requirements that apply to Kering.

The HR Department

The HR Department is responsible for communicating to Kering Users this GISP (induction pack) and for defining and communicating the disciplinary process/sanctions applicable to employees who have violated (committed an Information Security breach).

The Regional Security Correspondents

Regarding operational security, the CISO has regional security correspondents in Europe, Asia and the United States. They are responsible for implementing security objectives and principles defined herein and in the Operational Policies in their geographical perimeter.

Users, all actors of operational security

The protection of Kering Information is everyone's responsibility. Consequently, all Kering Users must demonstrate exemplary behavior in the protection of Information, values and work equipment in order to preserve the trust of Brands customers and achieve the Group's business objectives.

Managers: specific security responsibilities

Managers should ensure their team are security savvy and verify and demonstrate that their activities comply with the GISP principles.

Third Parties

Third Party Service Providers (individual consultants, subcontractors or suppliers, including their staff whether employee or not) must observe this GISP when accessing the Information or the Information System. They may also be required to implement additional security requirements.

6.2. Information Security Committees

The governance related to Information Security will be ensured by several committees, as follows:

Group Cybersecurity Committee: Quarterly security meeting with company executives

Gucci Cybersecurity Committee: Quarterly security meeting with Gucci company executives

Management Information Services Cybersecurity Committee (for brands): Quarterly security meeting with Brands & Houses

Kering Technologies and Digital Cybersecurity Committee: Quarterly security meeting with Kering Technologies and Digital Directors. The meeting takes place during Leadership team meeting.

Risk Committee: Quarterly risk meeting.

Audit Committee: Annual meeting dedicated to report on cybersecurity maturity.

6.3. Risk Management Integration

Risk management is a cornerstone of Kering's information security governance. It enables the identification, evaluation, and treatment of security risks in alignment with the organization's risk appetite.

- **Risk Identification**: Security risks are identified through assessments, threat intelligence, and audit findings.
- **Risk Assessment**: Risks are evaluated based on impact and likelihood using qualitative or quantitative methods.
- **Risk Treatment**: Controls are selected to mitigate, transfer, avoid, or accept identified risks.
- **Risk Reporting**: Significant risks are escalated to the Risk Committee and Executive Management.
- **Alignment**: Cyber risks are integrated into the broader Enterprise Risk Management (ERM) framework.

6.4. Security Control Framework

Kering applies a structured set of administrative, technical, and physical controls to ensure the confidentiality, integrity, and availability of its information assets. These controls are directly derived from international standards and frameworks and are selected as risk treatment measures based on the results of the organization's risk assessments.

- **Control Catalog**: Based on ISO/IEC 27001, ISO/IEC 27002, and NIST CSF, adapted to Kering's context and risk landscape.
- **Control Objectives**: Each control is aligned with specific risk scenarios to reduce the likelihood or impact of threats.
- **Implementation**: Controls are deployed through domain-specific operational policies and are consistently applied across systems and business units.
- **Control Ownership**: Responsibilities for implementing and monitoring controls are assigned to designated technical and business owners under the coordination of the CISO.
- **Continuous Improvement**: Control effectiveness is evaluated through audits, monitoring activities, and lessons learned from incidents. Controls are revised and strengthened as risks evolve.

These controls serve as the primary means to reduce security risks to acceptable levels, ensuring that the organization meets both its internal security objectives and external compliance requirements.
Kering applies a structured set of administrative, technical, and physical controls to ensure the confidentiality, integrity, and availability of its information assets.

6.5. Information Security Documentation Hierarchy.

Kering's Information Security Management System follows a structured three-level documentation approach that ensures comprehensive coverage while maintaining operational clarity. All cybersecurity policies, procedures, and work instructions are available in Kering Cybersecurity Portal.

Level 1: Global Information Security Policy

- This document serves as the master policy establishing strategic direction, governance structure, and overarching principles for information security across Kering Group
- Provides executive commitment and high-level framework
- Defines scope, objectives, and organizational context
-

Level 2: Functional Policies

- Domain-specific policies addressing particular security areas based on industry standards and frameworks
- Each policy incorporates control objectives from relevant standards and adapts them to Kering's business context
- Detailed in Section 6.6 of this document

Level 3: Procedures and work instructions

- Detailed implementation guidance describing how each security control is operationalized
- Step-by-step procedures ensuring consistent implementation across all Kering locations and business units
- Technical configurations and operational workflows

6.6. Functional Policies

Each functional policy is mapped to relevant industry standards and frameworks, incorporating their control objectives:

Security Domain	Policy Document	Source Standards/Frameworks	Key Control Objectives	Policy link
Artificial Intelligence and Autonomous Technology	**AAT**	EU AI Act, NIST AI Risk Management Framework (RMF), ISO/IEC 42001		AI Security Policy
Identity & Access Management	**IAM**	ISO 27002 (A.9), NIST CSF (PR.AC) / SCF IAC	User access provisioning, privileged access management, access reviews	
Data Classification & Handling	**DCH**	ISO 27002 (A.5.12, A.5.13, A.5.14, A.8.10, A.8.11), GDPR, NIST CSF (PR.DS)	Data classification, encryption, privacy by design, cross-border transfers	Data Access and Management Policy
Incident Response	**IRO**	ISO 27002 (A.16), NIST CSF (RS, RC)	Incident detection, response procedures, forensics, recovery	Cyber Incident Management Policy
Security Awareness & Training	**SAT**	ISO 27002 (A.6.3), NIST CSF (PR.AT)	Security awareness, training programs, competency development	
Endpoint Security	**END**	ISO 27002 (A.8.1, A.8.2, A.8.7)	Endpoint protection, device management, mobile security	
Risk Management	**RSK**	ISO 27002 (A.5.2, A.5.4, A.5.35)	Risk assessment, treatment, monitoring, reporting	Risk Management Policy
Threat Management	**THM**	ISO 27002 (A.12), NIST CSF (DE.CM)	Threat intelligence, hunting, analysis, response	
Vulnerability & Patch Management	**VPM**	ISO 27002 (A.12.6), NIST CSF (DE.CM)	Vulnerability scanning, patch management, remediation	Vulnerability and Patch Management Policy
Third Party Management	**TPM**		Assess third-party security posture	Supplier Risk Management Policy

			Include contractual clauses	
Continuous Monitoring	**MON**	ISO 27002 A.8.15, A.8.16, A.5.7	Real-time monitoring, log analysis, security analytics	IT Log Policy
Crisis Management	**CMG**		Crisis criterias, escalation	Crisis Management Policy

6.7. Communication

The GISP is available to all Kering users (internal and external) via the Kering Connect portal. It is also communicated to internal employees upon joining the Group.

Extract of GISP is included in Provider Security Requirement and is to be sent to Third Parties.

The related Operational Policies are classified as internal and made available to Users accessing Kering IT systems in Kering Cybersecurity portal.

7. Reporting and Escalation Procedures

All employees and contractors must report any observed or suspected information security incidents, policy violations, or weaknesses using the established internal procedures: **security@kering.com.**

If you need to report a security incident, request a penetration test, seek a security advisory, integrate security into projects, or ask for a contract review, you can send your request to: **Help Cybersecurity - Kering Connect**.

Security incidents are classified by severity and escalated according to predefined incident response workflows, ensuring prompt decision-making and appropriate involvement of stakeholders.

High-risk or major incidents are escalated to the CISO, who informs the Executive Committee, Risk Committee, and other relevant bodies as necessary. Incident response actions are coordinated in accordance with the organization's Incident Response Plan (IRP) and include root cause analysis, containment, and post-incident review. (See also: Cyber Incident Management Policy).

8. Kering's Information Security Principles

This policy applies to all employees, contractors, interns, and third-party personnel who access the information systems of Kering SA and its affiliates. It aims to ensure the confidentiality, integrity, and availability of information assets through clearly defined rules and security practices.

8.1. Responsibilities

All collaborators are expected to:

- Preserve the confidentiality and integrity of sensitive and personal data
- Use IT systems in accordance with internal policies and applicable regulations
- Report security incidents or anomalies without delay
- Apply security procedures and participate in awareness activities

8.2. Acceptable Use of IT Resources

Information systems and equipment must be used for authorized professional purposes only.
It is strictly prohibited to:

- Install or use unauthorized software or tools
- Connect unapproved external devices (e.g., USB drives)
- Access or store illegal, offensive, or hacked content
- Use company systems for personal commercial purposes

(See : Kering IT Charter)

8.3. Access Control and Password Protection

- Individual accounts must remain strictly personal and confidential
- Access to systems must be based on the principle of least privilege and role-based access control (RBAC)
- Passwords must follow defined complexity requirements
- Workstations must be locked when unattended
- Multi-factor authentication (MFA) is required for remote or sensitive system access

(See : Password Policy.pdf)

8.4. Data Protection and Confidentiality

- All personal and confidential information must be handled securely and only shared with authorized individuals through approved communication channels.
- Compliance with applicable data protection regulations (e.g., GDPR, PIPL) is mandatory.
- Documents and files must be labeled and managed according to internal data classification guidelines.

Kering implements a five-tier information classification system designed to ensure appropriate protection measures are applied throughout the information lifecycle:

Classification level	Description	Examples	Impact value based on risk ladder
Public	Documents which can be shared openly and with the public.Reserved for Kering Official external communications.	- Press releases - Published financial reports - Files downloaded from the internet	0-1
Internal	Documents relating to Kering or its Houses which can be shared with any Kering Group employee, contractor or partner.	- Internal communications - Internal presentations	2
Confidential	Documents whose handling is restricted to specific Kering Group employees, contractors or partners qualified to deal with them.)	- Employee performance and management - Payslips & tax documents - CRM - Strategic contracts	3
Secret	Highly sensitive documents that can be shared with only a very limited number of Kering Group employees, contractors or partners.	- Merger and acquisition information - Criminal investigations - Banking information	4

(See : Data Access and Management Policy)

8.5. Training and Awareness

- All personnel must complete mandatory cybersecurity training during onboarding and annually thereafter
- Security awareness campaigns (e.g., phishing simulations, posters) must be conducted regularly
- Specialized training must be provided for high-risk roles (e.g., system admins, golden rules)

8.6. Integration of Security in Projects

- Information security requirements must be systematically considered in all business and IT projects from the earliest planning phases.

- Risk assessments must be conducted for new systems or significant changes to existing systems.
- Security-by-design and privacy-by-design principles must be applied throughout the project lifecycle.
- Projects involving sensitive data or critical systems must include validation from the Information Security team.

8.7. Integration of Security in Contracts with third parties

- All third-party contracts must include relevant information security and data protection clauses, including confidentiality, access control, and audit rights.
- The level of security required must be proportional to the classification of data or services concerned.
- Security requirements must be aligned with internal policies and applicable legal/regulatory obligations.
- The Information Security team must validate contract clauses for high-risk suppliers.

8.8. Physical and Environmental Security

- Facilities must be secured with appropriate physical access controls (e.g., badges, biometric readers)
- Visitors must be registered and escorted
- Server rooms must be protected from environmental hazards such as fire, flood, or power loss
- Equipment must be disposed of securely to avoid data leakage

8.9. Network and System Security

- Firewalls, anti-malware, IDS/IPS systems must be in place and regularly updated
- Network segmentation is required to isolate sensitive zones
- All systems must be hardened and patched against known vulnerabilities
- Only secure protocols should be used for communication (e.g., HTTPS, SSH)

8.10. Monitoring and Logging

- Security events and user activities must be logged and stored securely
- Logs must be protected from unauthorized access or modification
- SIEM tools should be used to detect and respond to anomalies and threats in real-time
- Regular audits must be performed to verify log integrity

(See : IT Log Policy)

8.11. Incident Management

- A formal incident response process must be followed, including detection, classification, response, and recovery
- Incidents must be reported through designated channels
- Critical incidents must be escalated to the CISO and executive leadership
- Root cause analysis and post-incident reviews must be conducted

(See: Cyber Incident Management Policy)

8.12. Business continuity and Disaster Recovery

- Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) must be documented, approved, and tested regularly
- Systems supporting critical operations must meet established RTO and RPO thresholds
- Backup and recovery procedures must ensure data availability in case of disruption

8.13. Policy Review and Maintenance

- The policy must be reviewed annually or following major incidents, regulatory updates, or technological changes

- All changes must be documented and approved by the Information Security Governance Committee
- The latest version must be published and communicated to all stakeholders

8.14. Acknowledgment and Acceptance

- Personnel must acknowledge the policy as part of their onboarding process
- Periodic re-acknowledgment may be required after significant updates

9. Enforcement, Acknowledgment and Exceptions

9.1. Deviations and Exceptions

Any deviations from or exceptions to this Policy and the information security principles and security requirements contained herein, will require the written approval of the CISO.

9.2. Violations and Disciplinary Actions

- Violations will be investigated by the appropriate authority (HR, Legal, Security)
- Disciplinary actions may include warnings, suspension of access, termination, or legal action, depending on the severity and intent

10. Glossary

10.1. Acronyms used in the GISP

CISO	Chief Information Security Officer
GISP	Global Information Security Policy
IS	Information Systems
IT	Information Technology

10.2. Definitions

Affiliates	means in relation to Kering SA, any company or other legal entity, domestic or foreign directly or indirectly controlling, controlled by or under common control with Kering SA. "control" for the purposes of this definition means an ownership of at least 50% of the outstanding voting shares, powers or securities. The term "Affiliates" includes Kering Brands.
Kering Brands	means Kering Luxury Brands and Kering Sport and Lifestyle Brands (a full list of Kering Brands is available on http://www.kering.com).
Classification	means an operation which consists in defining the level of sensitivity of an Information according to one or more security criteria.
Confidential Information	means all information or data that is nonpublic, confidential or proprietary to Kering, whether in writing, oral, electronic, visual or other form, and including without limitations information concerning the business and affairs of any Kering Group company, its know-how, trade secrets, production information, sources of supply, products characteristics and specifications, current and planned distribution methods and processes, customer lists, Personal Ddata ,including the personal data of customers, suppliers and employees' of Kering SA and its Affiliates), price lists, financial information and any other financial, legal, commercial, marketing, organizational or technical information concerning the business and affairs of Kering SA or its Affiliates.
Equipment	means computers (desktops and laptops), personal digital assistants, cell phones, tablets, peripheral devices (keyboards, mice, USB flash drives, etc.), land-line telephones, telephone exchanges, portable data storage devices, photocopiers, printers and scanners, fax machines, e-fax systems, video-conferencing systems, third party networking services etc. In general, all other equipment used to ensure

	connections, service quality and the security of information and communication systems, including those wholly or partially run on behalf of Kering by third parties or all other similar items commonly understood to be covered by this term.
Information	means Personal Data, Confidential Information and any other information or data written, printed on paper or in electronic form, that is processed on or transits the Information System
Information Security	means the preservation of confidentiality, integrity and availability of Information.
Information Systems or "IS"	means all Equipment, software, applications, network and communications facilities, information repositories, and all equipment made available by or authorized by any Kering Group Company to Kering Users and used to collect, process, store, share and transfer Information
Kering or Kering Group	means Kering SA and its Affiliates.
Kering Service Providers	means individual or legal entities that provide services to Kering (including their staff whether employees or not) and may be granted access to or authorized to use the Information Systems to conduct Kering business.
Kering SA	means the corporation ("société anonyme") incorporated under the laws of France with registered address at 40, rue de Sèvres, 75007 Paris and company registration number Paris 552 075 020.
Kering's Top Management	The top management of Kering is composed by Kering Group deputy CEO, COO, CIO, General Counsel and Internal Audit Director.
"Kering Users"	means all individual working with or for Kering or its Affiliates, regardless of their status, including notably employees (permanent, temporary, full-time, part-time, home workers), individuals hired through staffing agencies, trainees and interns, executives, members of Kering or its Affiliates' boards), who are granted access to or authorized to use the Information Systems to conduct Kering business.
Personal Data	means any information, as defined in the applicable data protection laws, that can be used to identify Kering Users and Kering customers, suppliers, business partners and others. This includes, without limitations, any one or more of an individual's: (i) first and last name; (ii) home or other physical address (including a professional address); (iii) telephone numbers (landline or mobile, private or professional); (iv) email address(es) or other online contact information, such as an instant messaging user identifier; (v) title, (vi) IP address or other device identifier
Risk	Means a combination of the probalility of an event and its consequence. "Risk" is generally used when there is at least the possibility of negative consequences. In certain situations, the risk results from the possibility of a deviation with respect to the expected result or event.
Security Incident	means an event potentially affecting the confidentiality, integrity or availability of the Information System.
Social Engineering	means an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures to retrieve Information.

Gucci • Saint Laurent • Bottega Veneta • Balenciaga • McQueen • Brioni
Boucheron • Pomellato • Dodo • Qeelin • Ginori 1735 • Kering Eyewear • Kering Beauté

CONTACT

security@kering.com