Information Security Policy

Key information

1. **Policy owner** – Information Security & Risk Director
2. **Policy status** – **mandatory** for all directors and colleagues of Kingfisher plc (the "Company") and its subsidiaries.
3. **Policy adopted** – by GE
4. **Policy validation** – by the Information Security & Risk Director on 12th July 2021

Policy vision

At Kingfisher, we are committed to ensure that we manage *information* securely. This is part of our responsibility to our customers, colleagues, partner organisations, contracted third parties and shareholders. This means that all *information* processed, transmitted, or stored, both within Kingfisher and sent externally, must be secured, to protect against breaches of confidentiality, breaches of law, failures of integrity, and to ensure the information is available when it is needed.

Any deviation from, or exceptions to, this Policy must be risk assessed with the Information Security and Risk team.

Definitions of ***italicised*** words are set out in the Definitions section later in this Policy.

Contents

The policy

1.This policy applies to everyone who has access to Kingfisher ***information*** and **information systems** or services. This includes all colleagues, contractors, company partners and suppliers who are given access to Kingfisher ***information***.

2.This policy applies to all ***information*** processed by Kingfisher, or a third party on our behalf and includes:

- ***Information*** in both electronic and hard copy form
- ***Information*** hosted on both internal and external systems
- ***Information*** transmitted over internal and external networks.

3.Kingfisher is committed to applying the core principles of ***information security*** to protect our company, customer, and colleagues' ***information*** by:

- Taking a holistic and consistent approach to ***information security*** and applying that approach across Kingfisher and its contractors, partners, and suppliers, in line with agreed Company policies and standards, and in compliance with all relevant laws, regulations and contractual obligations
- Managing ***information security*** risks effectively, collectively, and consistently to ensure the confidentiality and integrity of the **information**, and that it is available to support business objectives and corporate values
- Minimising the risk to **information** processed, shared, and stored by ensuring that the ***information*** remains reliable, available, and protected against attacks and malicious activity, as well as recoverable in the event of an ***incident***. Additionally, all ***information*** will be destroyed securely when no longer needed.
- Implementing policies, standards, procedures, and controls to protect Company ***information***, and changes to the ***information systems*** implemented within the

organisation. These measures will be reviewed, approved, revised, communication and monitored to ensure they are adequate, effective, and sustainable for Kingfisher.

- Ensuring that everyone who processes Kingfisher ***information*** is made aware of this Policy and their responsibilities: personally, ethically, and professionally and the appropriate behaviours and controls required to protect Kingfisher's ***information*** from threats to the confidentiality, integrity, and availability of that information.

The process (replaces operating standard)

Information Ownership

- A record must be kept of ***information*** and where it is processed. Knowledge of where ***information*** is processed within the organisation will help to ensure that all ***information*** is appropriately maintained.
- ***Personal Data*** processing must be in line with the requirements of the Data Protection Policy.
- All ***information systems*** must be given an owner which can be an individual or a group of people who have been officially designated as accountable for specifically how that ***data*** is used, transmitted, stored on a system or systems.
- The Banners owns the ***data*** content and its governance, Group Technology own the ***technology framework*** in which the ***data*** is managed
- The ***Information Owner*** should be a manager within the team that relies on the ***data*** to support its business objectives. If multiple teams rely on the *data*, then the most appropriate senior manager should take ownership.
- The ***Information Owner*** for ***information*** should be recorded and will be involved in any decisions made regarding the treatment of the ***information*** when taken outside of a controlled systems environment, e.g., the need to export a large amount of ***data*** out of the controlled system to send to an external resource, is that appropriate and does the business agree to send the data

Information Classification

- All ***data*** must be classified according to Kingfisher Group Information Classification Policy.

Information Labelling

- Where applicable, ***data*** should be labelled according to Kingfisher Group Information Classification Policy All ***information*** in the form of documents including reports, presentations, spreadsheets etc. must be labelled to identify the sensitivity of the document.
- Authors are responsible for assigning a classification category to the documents they create if the contents are more sensitive than a public document. All documents will be considered internal as a default unless the document owner adds a classification proactively marking the contents as Confidential.

Secure Information Processing

- ***Information*** should be processed in line with the Security Standards
- Requirements for segregation of duty need to be considered, where different roles perform different tasks on ***data***. For example, the same person should not create a requisition and approve a vendor invoice
- Accountable business owners must have appropriate access to maintain ***data*** themselves
- ***Information*** should be mastered in single sources that are secure, maintained, current and appropriately accessible
- ***Data*** may need to be mastered in multiple systems but only where the data lifecycle requires that it is transferred from one system to another.
- ***Personal*** *data* may only be processed under the lawful basis for which it was collected and in line with the Data Protection Standard and Data Retention Standards.

Information Risk and Control Assessments

- Once the ***information*** has been identified we must ensure that the controls in place to protect that ***information*** meets the needs of the Information Security Standards.
- All ***information*** should exist either within a structure Service or System, however ***information*** can also exist in unstructured forms such as spreadsheets or documents held on file shares outside of a structure system.
- A ***controls assessment*** should be performed to identify where the controls protecting the Information do not meet the Standards. Where a control weakness is identified it must be registered in the Risk Register.
- Once identified, the risk to the business must be established by performing a risk assessment. Once the risk level has been established then the Risk Owner must decide on

the way to treat the risk and the appropriate timeframe to take to address the risk. The decision of risk treatment across technology systems is tracked via the Group Technology Risk Register.

Information and Third Parties

- It is important that ***information*** processed and / or stored by a third party is assessed and treated in the same way as if the ***information*** remained internally.
- ***Information*** should only be shared with third parties in accordance with the contracted services.
- If ***personal data*** is transferred it must comply with the requirements of the General Data Protection Regulation (GDPR).
- If a third party is processing card payments it must comply with Payment Card Industry Data Security Standard (PCI DSS).

Clear Desk and Screen

- All ***confidential information*** – on paper, a storage device or hardware - must be properly locked away or disposed of when a workspace is not in use.
- Colleagues and contractors must ensure that all ***confidential information*** in hardcopy or electronic form is secured.
- Computers must be locked from unauthorised access when workspace is unoccupied.
- Any ***confidential information*** must be removed from the desk and secured when the desk is unoccupied and at the end of the working day.
- Filing cabinets containing ***confidential information*** must be kept closed and locked when not in use or when not attended.
- Keys used for access to ***confidential information*** must not be left unattended.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing ***confidential information*** should be immediately removed from the printer.
- Upon disposal, confidential documents should be shredded by a cross-cut shredder or placed in the office locked confidential disposal bins. Under no circumstances should this information be placed in regular bins.
- Whiteboards containing ***confidential information*** should be erased.
- Lock away portable computing devices such as laptops and tablets.

- Treat mass storage devices such as CDROM, DVD or USB drives as confidential and secure them appropriately.

Bringing our policies to life

We all have a part to play in implementing these policies and supporting our culture. So, you should be aware that breaches of this policy may result in an investigation that could lead to disciplinary action, up to and including dismissal. Depending on the circumstances, such breaches may also constitute a civil and/or criminal offence.

Support and questions

If you have any questions about this Policy, or if you are uncertain how to apply or follow the process you can email InfoSec@kingfisher.com

Definitions

For the purposes of this Policy:

Confidential information is information that is confidential to Kingfisher and the Banners, for example sensitive business information, the personal data of our customers and colleagues, cardholder data.

Data is an asset that is owned by Kingfisher and/or the Banner. We rely on data to be able to function as a business. Examples of data include product, commercial, financial, brand and personal data. Data is used interchangeably with ***information*** in this policy.

Incident is an instance of something happening resulting in information not being available, being compromised or disclosed where it should not have been.

Information is an asset that is owned by Kingfisher and/or the Banners. We rely on information to be able to function. Examples of information include product, commercial, financial, brand and personal information. Information is used interchangeably with ***data*** in this policy

Information owner is a Kingfisher or Banner colleague who is accountable for specific information

Information security is the protection of our information and information systems from unauthorised access, use, changes, disclosure, disruption, or destruction and to ensure it remains available and accurate to those colleagues who are authorised to access it.

Information systems are the technology solutions and software that help us organise, store, and analyse our data

Personal data is information that relates to an identified or identifiable person

Related documents

- Data Protection Policy
  Data_Protection_Policy.pdf (sharepoint.com)
- Access Control Standard
  Information Security Standards (sharepoint.com)
- Cloud Security Standard
  Information Security Standards (sharepoint.com)
- Information Classification Policy
  our policies and colleague guides (sharepoint.com)
- Network Security Standard
  Information Security Standards (sharepoint.com)
- Operational Security Standard
  Information Security Standards (sharepoint.com)
- Physical & Environmental Standard
  Information Security Standards (sharepoint.com)
- Systems Development Standard
  Information Security Standards (sharepoint.com)