Information Security Policy

October 2026

POLICY STATEMENT

This policy sets out how Brigantia Partners Ltd trading as Elovade UK&I has organised itself to identify potential threats to the confidentiality, integrity and availability of the data and information that the company manages or is custodian of, and how it undertakes to mitigate those threats and maintain the security of this information.

Regular reviews and audits of the Information Security Management System are undertaken to ensure that the system is continually improved.

This policy identifies the underlying policies that Elovade UK&I deploys and how it ensures that those policies and the accompanying processes, procedures and activities are maintained, managed and reviewed to ensure that they remain fit for purpose and that the impact of information security incidents is minimised.

POLICY SCOPE

The scope of this policy encompasses all Elovade UK&I employees and vendors, and the information processed by them. It covers all operations, whether undertaken in or out of the office, and includes:

- All information processed by Elovade UK&I in pursuit of its operational activities, regardless of whether it is processed electronically or in paper form, including but not limited to:
    - Partner, Client and Vendor information
    - Information processed by the operational teams in the day-to-day delivery of Elovade UK&I's services and solutions
    - Accounting records
    - Management and meeting records
    - Employee records
- All information processing facilities used in support of these activities to store, process and transmit Information either for internal use or as part of a client service
- All information received from external organisations that provide services to Elovade UK&I.

This policy also applies to the management of the supply chain and requires vendors to maintain appropriate information security measures.

Elovade UK&I management requires this policy to be implemented to the fullest extent appropriate to ensure business continuity and minimise business damage by preventing information security incidents and minimising their impact.

INFORMATION SECURITY RESOURCING AND TRAINING

© Brigantia, Cloud Business and Enhance logos, and combinations thereof, are trademarks and trading styles of Brigantia Partners Limited. All rights reserved. Company No. 09498907.

The Elovade UK&I management team will ensure that the necessary resources to establish, implement, maintain and continually improve the information security of the business are identified and provided.

These resources shall include, but not be limited to:

- People
- Information and data
- Buildings and associated utilities
- Facilities and equipment
- Finance
- Partners
- Vendors and other interested parties.

The management team will ensure that an Information Security Manager is assigned responsibility for the adequacy of these measures.

This role will require that:

- All information security incidents or near misses are recorded, actioned and reviewed.
- When an incident is closed, a review is undertaken to ensure that any learning points are incorporated into the Information Security Management System.
- Regular reviews are undertaken to ensure this policy and all other information security-related policies remain fit for purpose and meet all legal, regulatory and contractual requirements.
- Regular education and training is undertaken to ensure that all employees are capable of meeting the information security requirements of their roles.
- All employees are aware of what they should do and how they should react if they become aware of an information security incident or near miss.

Everybody who is a member of the Elovade UK&I organisation will be educated in the need for information security, and this awareness will be refreshed across the whole organisation at least once every two years.

The security responsibilities of third parties shall be made clear, regularly monitored and reviewed as part of the management of vendor security responsibilities.

THREATS AND VULNERABILITIES TO INFORMATION SECURITY

Elovade UK&I has identified and maintains a key threat list that identifies the key vulnerabilities to the security of the company's information and data. This threat list will be applied to all information assets, using a repeatable risk assessment approach to ensure that identified threats are reduced to an acceptable level and that actions are in place to ensure the security of all information assets.

DATA CLASSIFICATION

All Information Assets will be classified according to their need for security. Each security classification will have defined means for how these Information Assets are handled, managed, communicated and disposed of to ensure that they remain secure.

© Brigantia, Cloud Business and Enhance logos, and combinations thereof, are trademarks and trading styles of Brigantia Partners Limited. All rights reserved. Company No. 09498907.

RISK MANAGEMENT

Elovade UK&I uses a risk management approach to support the implementation, development and maintenance of information security policies and the protection of information assets.

The risk management approach will be repeatable to ensure that all assets are adequately protected. Risk assessments will be performed before and after any significant change in the business environment (i.e. a significant change to people, processes or technology), or when a weakness, new threat or vulnerability to a policy or other control has been identified.

All risk assessments will result in risk treatment plans to ensure that identified risks are treated to bring them within acceptable business parameters. All results will be submitted to the Information Security Review for assessment and validation.

NETWORK SECURITY AND MONITORING

External access to Elovade UK&I's systems is necessary for the smooth operation of the business. Therefore, access to these networks and network services must be protected.

This is achieved through ensuring that:

- All ports that are not actively required for inbound or outbound traffic are blocked against unauthorised access.
- Default passwords and factory settings are changed on network management devices.
- Appropriate interfaces and agreed security protocols are in place between Elovade UK&I's networks and public networks or networks owned by other organisations.
- Users are only provided with access to services that they have been specifically authorised to use.
- Appropriate authentication mechanisms are used to verify users and devices accessing company systems and services.
- Network and system activity is monitored using appropriate security tools, with alerts investigated where suspicious activity or potential security incidents are identified.

MALWARE PROTECTION

Software and information processing facilities are vulnerable to the introduction of malware, such as computer viruses, network worms, trojans and logic bombs. Elovade UK&I protects its systems and operations against these threats through the use of malware detection and prevention software, appropriate system access and change management controls, and information security awareness training for staff.

These protections include:

- Prohibiting the use of unauthorised software.

© Brigantia, Cloud Business and Enhance logos, and combinations thereof, are trademarks and trading styles of Brigantia Partners Limited. All rights reserved. Company No. 09498907.

- Ensuring that software downloads and installations are restricted to authorised individuals and appropriately controlled.
- Ensuring that data is transferred using authorised and agreed protocols and systems.
- Ensuring that manually transferred data is checked for malware where appropriate.
- Scanning email attachments and downloads for malware using appropriate security controls.
- Conducting regular reviews of the software and data held on systems and investigating the presence of unapproved files or unauthorised amendments where identified.
- Installing and regularly updating malware detection and prevention software to protect computers and other relevant devices.
- Regularly installing security patches and upgrades as they become available, in accordance with the applicable patch management process.
- Keeping informed about emerging malware threats and taking appropriate action where necessary.

ACCESS CONTROLS

Access to Elovade UK&I's information and systems is controlled through a combination of physical security, system access controls and device security measures.

- Access to physical locations is restricted to individuals who are authorised to access those locations.
- User access to systems is controlled through authorised user accounts, unique user identities and appropriate authentication mechanisms.
- User access permissions are reviewed regularly to ensure that access remains appropriate and that only authorised individuals retain access to company systems and information.
- Administrative access to systems is controlled through appropriate privileged access controls, including separate administrative accounts where required.

USE OF REMOVEABLE MEDIA

The use of removable media, including USB drives and memory sticks, is prohibited for the storage or transfer of company information unless specifically authorised for a legitimate business purpose and subject to appropriate security controls.

MOBILE EQUIPMENT

Company-owned mobile equipment, including laptops, must be managed securely to protect the equipment and the information stored on it.

All company-owned mobile equipment issued to employees must be recorded in the company's Information Asset Register or other appropriate asset records.

Users are responsible for taking reasonable precautions to prevent the loss, theft or unauthorised use of company-owned mobile equipment. Devices must be kept secure when unattended and must not be left in locations where they are at unnecessary risk of loss or theft.

© Brigantia, Cloud Business and Enhance logos, and combinations thereof, are trademarks and trading styles of Brigantia Partners Limited. All rights reserved. Company No. 09498907.

Company information stored on mobile equipment must be protected using appropriate security measures, including encryption where required. Information stored locally on devices should be kept to the minimum necessary for business purposes and removed when no longer required, where appropriate.

Company-owned mobile equipment must be returned when an individual's employment or engagement with the company ends, or when otherwise requested.

HOME WORKING

Employees may work from home or other remote locations where authorised and where appropriate to their role and business requirements. This includes the use of company equipment and access to company information outside the office.

Users must ensure that company information is protected when working remotely. Connections to company systems and services must use appropriate security measures, including secure network connections and approved remote access methods where applicable.

Company information must be handled securely and protected against unauthorised access, loss or disclosure, regardless of the user's working location.

The use of personal devices to access company information is subject to the requirements of the Bring Your Own Device Policy (BYOD).

INCIDENT MANAGEMENT

All individuals working for Elovade UK&I on company-sanctioned activities are responsible for reporting any information security event they identify. All such events must be reported to the Information Security Manager as soon as reasonably possible after they are identified. Both incidents — actual breaches of information security policies — and near misses — potential security incidents — must be reported.

All reported incidents and near misses must be investigated within a reasonable timescale, and any necessary resolution activities identified and implemented. Where an investigation identifies opportunities for preventative action or improvement, these must also be considered and actioned as appropriate.

Appropriate backup arrangements are maintained to support the recovery of company information and systems in the event of data loss or a disruption to services.

In the event of a critical incident that prevents the business from continuing to provide services to its partners and clients, recovery arrangements, including the restoration of available backups and the implementation of applicable disaster recovery and business continuity plans, will support the restoration of normal business operations.

RESPONSIBILITIES

The Information Security Manager is responsible for ensuring that this policy is maintained, reviewed and updated as necessary.

© Brigantia, Cloud Business and Enhance logos, and combinations thereof, are trademarks and trading styles of Brigantia Partners Limited. All rights reserved. Company No. 09498907.

ELOVADE

Reviews shall be completed in accordance with the Document Control Policy.

© Brigantia, Cloud Business and Enhance logos, and combinations thereof, are trademarks and trading styles of Brigantia Partners Limited. All rights reserved. Company No. 09498907.