Information Security Policy

August 2022

Policy Statement

This policy sets out how Brigantia 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 continue to ensure the safety of this information. Regular reviews and audits of all areas of the Information Security Management System are undertaken to ensure that the system is continuously improved.
This Policy identifies the underlying policies that Brigantia deploys and how it ensures that those policies and the accompanying processes, procedures and activities are maintained, managed and tuned to ensure that they remain fit for purpose and that the impact of information security incidents are minimised.

Policy Scope

The scope of this policy encompasses all Brigantia 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 Brigantia 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 Brigantia'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 Brigantia.

It also applies to the management of the supply chain and requires Vendors to ensure they operate appropriate information security measures.
The Brigantia management team require that this policy is deployed to the fullest extent to ensure business continuity, and minimise business damage by preventing the occurrence, and minimising the impact, of information security incidents.

Information Security Resourcing and Training

The Brigantia 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 will be assigned to be responsible 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 and able to meet 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 Brigantia organisation will be educated in the need for information security and that 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 regularly reviewed as part of these Vendor security responsibilities.

Threats and Vulnerabilities to Information Security

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

Risk Management

Brigantia uses a risk management approach to support the implementation, development and maintenance of security policies and information assets. The risk management approach will be repeatable to ensure that all assets are adequately protected. A risk assessment will be performed before and after any significant change in the business environment (i.e. a significant change to people, process or technology) or when a weakness, new threat or vulnerability to either a Policy or other control has been identified. All risk assessments will result in risk treatment plans to ensure all identified risks are mitigated 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 Brigantia's systems is necessary for the smooth operation of the business. Therefore, access to these networks and network services need to be protected.

This is achieved through ensuring:

- All ports that are not actively required for inbound or outbound traffic are blocked against unauthorised access
- Default passwords and factory settings are reconfigured on all network management devices
- Appropriate interfaces with agreed security protocols are in place between Brigantia's network 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.
- Active Directory is used to authenticate users and equipment

Malware Protection

Software and information processing facilities are vulnerable to the introduction of malware, such as computer viruses, network worms, trojans, and logic bombs. Brigantia protects itself and it's operations against these threats by using malicious code detection and repair software, appropriate system access and change management controls and will educate all staff in data security awareness.

These protections include:

- Prohibiting the use of unauthorised software
- Ensuring only authorised individuals are allowed to download software, and the monitoring of those downloads.
- Ensuring data is only transferred via authorised and agreed protocols and systems
- Ensuring manually transferred data is checked for malware before transfer is allowed to take place.
- Scanning electronic mail attachments and downloads for malware before being released to the user
- Conducting regular reviews of the software and data content of systems and investigating the presence of any unapproved files or unauthorized amendments
- Installing and regularly updating malware code detection and repair software to scan computers and media on a routine basis

- Regularly installing security patches and upgrades as they are released
- Regularly checking for information about new malicious code and appropriate responses if attacked.

Access Controls

Access to Brigantia's information and systems is controlled through a combination of controls on physical, system and device security.

- Access to physical locations is restricted to those individuals who are authorised to access those locations.
- User access to systems is controlled through the secure use of authorised user accounts with unique usernames and secure passwords
- System user lists are continuously reviewed to ensure that only those with current authorisations are allowed accounts
- Administrative access to systems is controlled through the secure use of segregated Admin accounts with separate username/ password combinations.

Use of Removeable Media

Removable media in the form of USB drives and memory sticks are not authorised for use in the delivery of Brigantia services.

Mobile Equipment

All company owned mobile equipment must be secured in a locked room or office during non-business hours or must be suitably managed by the individual responsible for the equipment. Any such equipment issued to an individual must be documented and a copy of this record filed in Brigantia's Information Asset Register. When the individual ceases to work for the Brigantia they must return the mobile equipment prior to the last day of employment.
To ensure security of the data contained on a mobile device all data must be saved directly to the encrypted area of the device. In addition, the stored data should be kept to a minimum and deleted when it is no longer needed as mobile or portable devices are not deemed suitable for long term storage of Brigantia data. Each user of a Brigantia owned mobile device is expected to keep it safe and to ensure that the device, and the data that it contains, are kept safe.

Home Working

Home working is limited to authorised members of staff who have a genuine business need. This covers all media and equipment except for that described in the Bring Your Own Device Policy (BYOD). Use of any information at home must be for work purposes only and connection must be via a cabled connection or using a suitable secured wireless connection or VPN.

Incident Management

All individuals working for Brigantia on company sanctioned activity are responsible for reporting any information security event that they notice. All such events must be reported to the Information Security Manager as soon as possible once they have been identified. Both 'incidents' – actual breaches of information security policies – or 'Near Misses' – potential events – must be reported.

All reported incidents and near misses must be investigated within a reasonable timescale and any resolution activity identified and implemented as necessary. In addition, should the investigation identify any potential preventative action, this must also be considered and actioned.

All Brigantia systems and data are backed up to ensure that should an incident occur that results in the loss of data, the data can be easily recovered.

In the event of a critical incident, resulting in the catastrophic failure of the business to continue servicing it's Partners and clients, the restoration of data backups, in conjunction with the actions defined in the Disaster Recovery Plan, will facilitate the efficient and effective return to normal working.

Responsibilities

The Information Security Officer is responsible for ensuring the maintenance and updating of this policy.

Reviewing process should be completed in line with the Policy Control and Management System.