



## INFORMATION SECURITY AND DATA PROTECTION POLICY

Information is one of Bravida's most important assets, and information management is a significant part of the company's work. We handle sensitive data about our business activities, our customers and other stakeholders on a daily basis. Access to reliable information is a must for allowing Bravida to continue to be successful and efficiently develop and deliver our services and products to customers in a sustainable and innovative way.

### **Purpose:**

The overall purpose of Bravida's information security and data protection procedures is to ensure suitably balanced protection of Bravida's information assets. The right information should be available to the right person at the right time. The personal data that Bravida handles is processed in accordance with applicable data protection legislation.

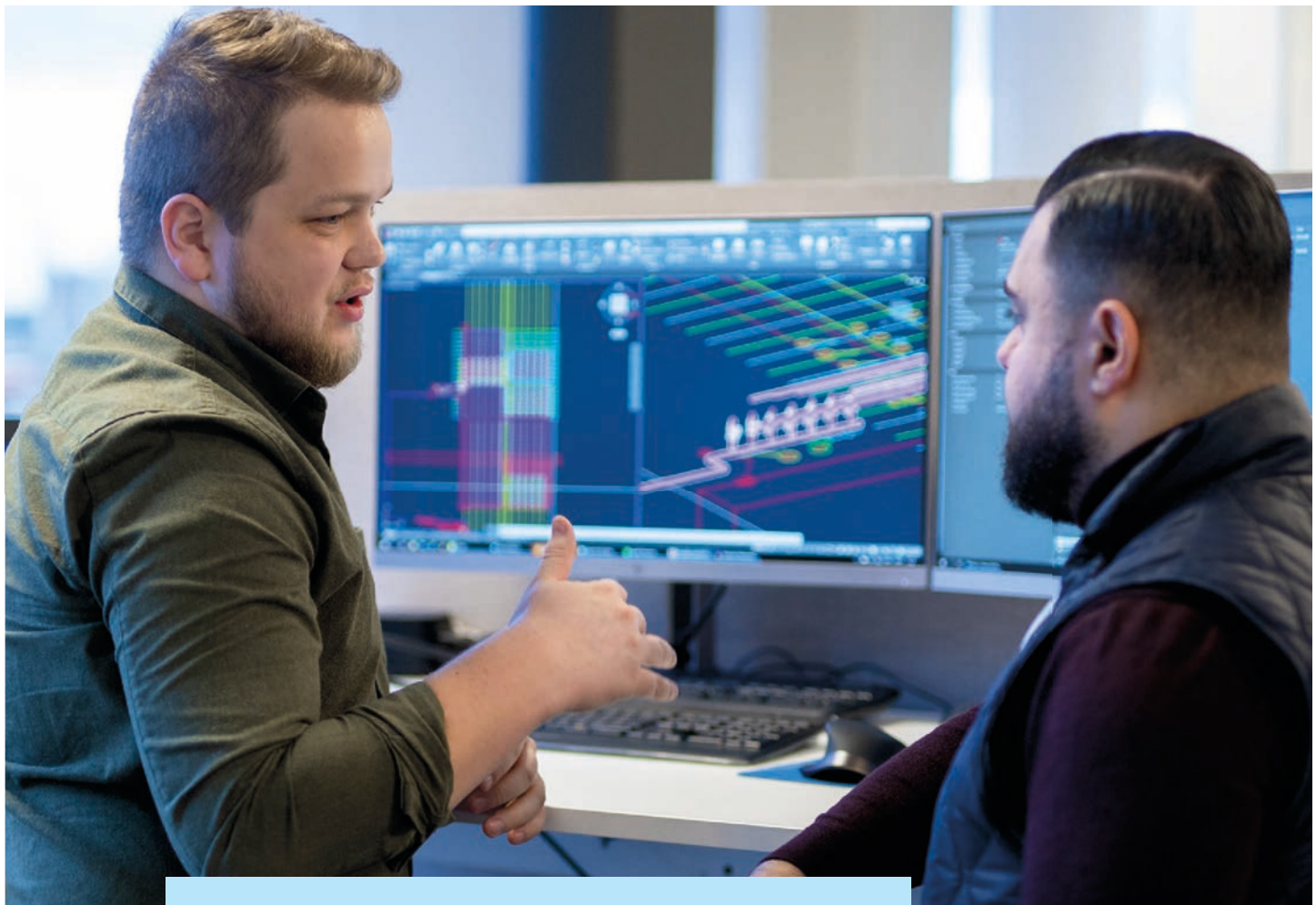
The systematic approach to information security and data protection ensures a robust, secure and reliable provision of information based on adequate protection and minimisation of risk. It also aims to prevent events that would have a negative impact on the ability to carry out effective business operations.

### **Scope:**

The policy covers the entire Bravida Group's business activities and all information without exception, regardless of whether it is processed manually or automatically and regardless of its form or the environment in which it exists. All sensitive information shall be classified according to its degree of sensitivity.

The policy is aimed at everyone who handles Bravida's information and describes the management's view and Bravida's guiding principles regarding information security and data protection.

The means of protection of information assets shall be designed to meet the security requirements of the business. This also applies when Bravida's information or information systems are utilised by an external party and when Bravida handles third party information.



### **Principles**

Bravida complies with regulatory requirements and good practice relating to information security and data protection.

### **Information security**

Bravida's work with information security and data protection must take a systematic and long-term approach with a holistic view, based on information, as well as processes, people and technology. The work is based on the established standard series SS-ISO/IEC 27000 and involves regular risk analyses aimed at achieving the right level of protection in all parts of the business.

### **The work with information security shall ensure:**

#### **CONFIDENTIALITY**

The information is not made available or disclosed to unauthorised individuals, entities or processes, or otherwise disclosed knowingly or unknowingly to anyone other than an authorised person.

#### **CORRECTNESS**

It is not possible for the information to be altered by unauthorised persons, by mistake or due to disruptions in IT systems or business operations. The information should be reliable, accurate and complete.

#### **ACCESSIBILITY**

The information should be accessible when needed, to the extent expected, at the right time and in the right place.





### Data protection

Responsible and systematic data protection practices. Bravida takes full responsibility for our processing of personal data and works in a systematic and structured way to ensure compliance with rules and established principles.

#### LEGALITY

All our processing of personal data is carried out in accordance with applicable laws and regulations and is characterised by Bravida's values and these guiding principles.

#### CORRECTNESS

All personal data collected and processed by Bravida shall be accurate and be updated if necessary.

#### OPENNESS AND TRANSPARENCY

Bravida shall always act openly and transparently and provide clear, accessible information about how we process personal data and the relevant rights of individuals.

#### LIMITATION OF PURPOSE

All our processing of personal data is carried out for explicit and legitimate purposes and we recognise that the stated purpose defines the limits for our processing of personal data in each case.

#### DATA MINIMISATION

We only process the personal data that is sufficient, relevant and necessary for fulfilling the stated purpose.

#### STORAGE MINIMISATION

We do not retain personal data for longer than is necessary to fulfil the stated purpose.

#### SECURITY AWARENESS AND DATA PROTECTION BY DESIGN

We safeguard the personal data we process and take appropriate technical and organisational security measures to protect the personal data.

For each of the areas in information security and data protection, a number of organisational, administrative and technical safeguards shall be implemented and documented in such a way that it is possible to verify that an adequate level of protection is achieved. Deviations should be detected, handled and provide a basis for improvement.

## Responsibility

The Board of Directors decides on the policy, the CEO has the ultimate responsibility and the responsibility for developing the area further is delegated to the CISO. The operational responsibility for information security follows the normal delegated business responsibility at all levels, and managers are responsible for implementing the content of this policy in their own part of the business.

Bravida's CEO is ultimately responsible for information security and for overall security issues that have a governing nature. This responsibility includes ensuring that financial and human resources with the right competences are available for carrying out information security work.

### EVERYONE WHO HANDLES BRAVIDA'S INFORMATION

- Everyone who handles Bravida's information has to be aware of their responsibilities and have good knowledge of the security rules that apply.
- People who handle Bravida's information shall regularly be given the necessary training to maintain information security and data protection.

### SERVICE MANAGER AND INFORMATION OWNER

- All IT services, and the equipment they include, are handled within the framework of Bravida's management model. The responsibilities from the governance model include ensuring compliance with the security requirements for the IT services.
- All sensitive information shall be allocated an owner. • The information owner is responsible for classifying the information and defining the security requirements necessary to ensure that the information is adequately protected.
- Based on regular risk and vulnerability analyses and incidents that have occurred, the Service Manager and information owner must take the necessary measures to ensure that Bravida's information assets have appropriate protection.

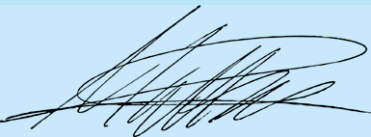
## Review and monitoring

Compliance with the Information Security and Data Protection Policy and related guidelines shall be monitored regularly, as shall the implemented safeguards. The results of the security work shall be reported annually in the management review.

The Information Security and Data Protection Policy and related regulations shall be reviewed and updated annually, or when significant changes in the organisation or framework conditions occur. This is to ensure the continued appropriateness, correctness and effectiveness of the policy.

The review shall include an assessment of Bravida's possibilities regarding improving its regulatory framework and the organisation's approach to information security and data protection, based on changes in the framework and environment within which Bravida exists, its operational conditions, legal requirements and technical aspects.

Bravida, 4 November 2024



Mattias Johansson, Group President and CEO

All policies are reviewed annually.