Brilliant

Brilliant General Information Security Policy

2022-06-01

Version 1.2

Classification: Public

Versionshantering

Version	Author	Approved by	Date	Description
1.0	Johan Pellbäck	Brilliant managment team	2022-06-01	New format and policy update, part of the ISO certification planning process
1.1	Johan Pellbäck	Brilliant management team	2022-10-06	Update and review
1.2	Johan Pellbäck	Brilliant management team	2024-08-26	Update risk management policy
1.3	Johan Pellbäck	Mattias Palmaer, Ulrika Frimmel, Jack Gilberg	2026-01-27	Added chapter 2, 3 regarding legal, regulatory, contractual and commercial requirements
1.4	Johan Pellbäck	Teet Sirotkin	2026-03-20	Added scope for ISMS, chapter 2

Brilliant

Content

Brilliant

1 Purpose

This policy defines the main principles regarding Information Security to ensure that Brilliant Future AB complies with applicable laws, regulations and ways of working throughout the organization external partners.

This policy regulates in a uniform way how Brilliant manages information security and is targeted to all personal, consultants and partners working for Brilliant and included entities.

This policy together with the complete ISMS shall address compliance with applicable legal, statutory, regulatory and contractual requirements related to information security, data protection and privacy.

2 Scope

This information security policy covers all employees, consultants, business areas, products, processes within the legal entities Brilliant Future AB (556392-3332), Brilliant Future Consulting AB (559502-8167) and Brilliant Future Sverige AB (556663-8762) and the head office at Drottninggatan 26 in Stockholm.

3 Legal and regulatory requirements

The following legal and regulatory frameworks are applicable to Brilliant Future AB and shall be complied with where relevant:

- **EU General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679**
  Including requirements related to lawful processing, security of processing (Art. 32), breach notification (Art. 33–34), data subject rights, DPIAs, and processor obligations.
- **Swedish Data Protection Act (Dataskyddslagen, SFS 2018:218)**
  Supplementary national legislation to GDPR.
- **EU AI Act (as applicable)**
  For use of AI-based features, including risk classification, transparency, and governance obligations.
- **NIS2 Directive (EU) 2022/2555 (as applicable)**
  Requirements related to cybersecurity risk management, incident reporting, and supply-chain security for essential and important entities.
- **Accounting Act (Bokföringslagen, SFS 1999:1078)**
  Retention and integrity requirements for financial and contractual records.
- **Companies Act (Aktiebolagslagen, SFS 2005:551)**
  Requirements related to corporate governance, internal control, accountability, and protection of company information
- **The Swedish Corporate Governance Code**

Principles and requirements related to governance structure, internal control, risk management, transparency, and accountability, as applicable to listed or growth-market companies.

- **Swedish Labor law and collective bargaining agreement**
  Including protection of employee-related personal and confidential information.
- **Applicable accessibility regulations**
  Including WCAG 2.1/2.2 requirements where contractually or legally required (e.g. public sector customers).
- **Nasdaq First North Growth Market – Rulebook for Issuers of Share**
  Principles and requirements related to governance structure, internal control, risk management, transparency, and accountability, as applicable to listed or growth-market companies.

4 Contractual and Commercial Requirements

Brilliant Future AB shall comply with information security and data protection obligations arising from contractual agreements, including but not limited to:

- **General terms and conditions**
  Including confidentiality, availability, integrity, incident handling, and security commitments
- Data Processing Agreements (DPA)
  Defining roles, instructions, security measures, sub-processing, breach notification timelines, and audit rights.
- Standard Contractual Clauses (SCCs)
  Where applicable for transfers of personal data outside the EU/EEA.
- Supplier and Sub-processor Agreements
  Including security requirements, confidentiality, audit rights, and compliance with applicable laws and standards.
- Service Level Agreements (SLAs)
  Covering availability, incident response times, support commitments, and reporting.
- Non-Disclosure Agreements (NDAs)
  With employees, contractors, partners, and third parties.

5 Policy Implementation and Compliance

The management team at Brilliant Future (through the CEO) is ultimately responsible and accountable for ensuring that objectives of this policy are met.

The CTO is responsible for the implementation of this policy and is authorized to pursue activities to achieve the policy objectives.

The DPO at Brilliant is responsible for regulating activities to achieve objectives part of this policy. This can from time to time be conducted by security- or legal partners to Brilliant Future.

6 Monitoring of Compliance

The CTO shall monitor the Policy in the following manner:

- Self-assessment evaluations include areas such as Information security, IT security and privacy in the yearly cycle.
- Monitoring of privacy shall be performed in accordance with applicable data protection legislation.
- To ensure compliance with data protection regulation Brilliant has appointed a Data Protection Officer.
- All managers shall be overall responsible for the compliance of the information security policy within their mandates and authorities and to ensure that all their subordinates are aware of and comply with it.
- All personnel and consultants within Brilliant, including entities, shall read, understand and accept this policy.
- New employees shall receive training as part of the introduction process. Training shall be provided on a regular basis and completion of training is compulsory.

7 Exceptions to this policy

Exceptions to this policy may during special circumstances occur and should be approved by the management team at Brilliant, as long as this does not deviate from laws and regulations.

8 Main principles

The IT information security policy and privacy governance shall contribute to the business goals by limiting the security and privacy risks to an acceptable level.

8.1 Information Security

Information security should protect operations, employees and customers by defining appropriate information security requirements based on applicable laws and legislations, good practice as well as employees and customer expectations. The requirements should ensure that correct information is available, when needed, to the intended persons only.

Confidentiality, integrity, and availability of information should be based upon appropriate parts of the ISO 27001 standard. The implementation and control of the standard is reflected in respective process documentation.

8.2 IT Security

IT security is an integrated part of Information Security and shall ensure appropriate protection of IT systems and IT infrastructure to achieve required protection level of information.

- IT Security requirements should be defined in relevant IT processes (such as incident management, development/SDLC, maintenance and support).
- Inventory of IT Systems and applications shall provide information about systems owners and data to enable effective IT security governance. The inventory indicates

business criticality and whether the application contains and/or handle personal data.
- Access control shall be used to ensure that only intended users have access to the system and information based on business needs. ID management shall be performed to ensure that user IDs and correspondent access rights (role management) are kept up to date.
- Systems (servers, services, applications) should be monitored and protected from DDOS attacks, malicious code, have access control, log functions, backup routines and appropriate security measures.
- The possibility of working remotely shall be enabled by appropriate security measures (such as encryption, MFA etc)
- Appropriate IT security measures shall be defined and applied when sourcing agreements are made, and it shall be possible to monitor compliance with external partners.
- Systems should be kept up to date with latest security updates including virus protection.
- Information and physical assets shall be registered.

8.3 Privacy
Brilliant Future shall comply with applicable data protection legislation to safeguard that private customer and employee privacy rights are not violated.

Brilliant Future shall follow appropriate routines and governance so that it can demonstrate compliance with relevant data protection legislation in case of an audit request from customers or Data Protection Authorities.

8.4 Incidents
In the event of identifying or being informed that the security of the processing of personal data has been compromised, or there has been any unauthorized or accidental disclosure of or access to personal data, Brilliant will inform the relevant data subjects or data controllers whose data may or have been compromised.

Furthermore, Brilliant should have in place specific procedures for how to handle a personal data breach incident, including how to notify the Data Protection Agency (IMY) according to EU general data protection regulation as well as relevant business continuity plans.

9 References

- Information Security for Employees (Encrypted internal)
- Brilliant Privacy Policy (Public)
- Brilliant Incident Management Process (Public)
- Brilliant Software Development Process (SDLC) (Confidential)
- Brilliant Business Continuity Plan (Confidential)
- Brilliant Risk Management Policy (Confidential)
- Together with other relevant process documents in ISMS