Betsson & Information Security – Policy summary

Protecting customer data and securing sensitive information

As a leading iGaming Operator, Betsson handles substantial amounts of sensitive information every day. Large parts of this information hold significant value, both to Betsson, but also to all our customers enjoying Betsson's wide range of online gaming experiences. Therefore, it is of utmost importance to make sure that this information is handled in a secure manner and that it is protected from misuse. The long-term information and cyber security strategy therefore focuses on activities aimed to protect information, reduce risk across all business areas, and prevent unwanted human behaviour, whilst protecting the creation of value, making it a core component of a continual improvement process. The goal is to achieve a mindset where security is built in by design, resulting in an overall better quality product offering, with security woven into the very fabric of its business operations.

This is further evidenced by Betsson's ISO27001 and PCI-DSS (Payment Card Industry Data Security Standard) certifications demonstrating its commitment to the protection of value. In addition, Betsson's Internal Auditor regularly conduct information security audits in agreement with the Board of Director's Audit Committee to assess and identify any areas which can be improved.

Information Security Objectives paving the way

The overall goal is to ensure execution of the strategy without undesirable human interference, whilst safeguarding that the Group reaches its strategic objectives and maintains good business performance. The Information Security objectives are outlined in the Group's Information Security policy (the "Policy"), approved by the Operational CEO. The Policy applies to information security management across the whole Group.

The Policy lists ten explicit Information Security Management System objectives which form the basis of the Group's endeavours within information security. These objectives include:

- the provision of a safe and secure gaming platform,
- the protection of customers' and Betsson's information,
- the identification and management of security risks in Betsson's supply chain,
- the training of staff on security and regulatory security requirements,
- security in recruitment processes,
- the diligent handling of security incidents,
- compliance with contractual and regulatory gaming requirements,
- the maintenance of industry standard certifications (ISO27001 and PCI-DSS),
- ongoing improvements when it comes to security governance, and
- continuous compliance with all other underlying Information Security policies.

In the form of statements, the Policy further lays down the need to maintain a full inventory of assets, and proper access management. This is complemented by statements, amongst others, around the need for media handling and information classification, as well as with the acceptable use of its assets and information across the Group.

The requirement for regular risk assessments covers the basis for the reduction of risk, whilst there is an emphasis on the need to handle security incidents with diligence and maintain a solid Business Continuity Framework - all enabling the Group to apply both proactive and reactive best practice measures when needed. Since Betsson is technology centric, the Policy specifies the need for secure development and the necessity to have proper physical and environmental security measures in place. Lastly, considering that Betsson is also a payment-service provider managing a card data environment since 2014, the Policy is instrumental in laying down the need to ensure that this environment is completely compliant with PCI-DSS security requirements.

Evidence of access control and protection of personal/sensitive data	**Data Breach/Incident Response Plan**
✓ Access control to our portals is always over secure encrypted links guaranteeing end-to-end encryption ✓ Web-application security controls are in place at a firewall level during login to prevent login abuse by bots ✓ Denial-of-service security controls are in place to ensure site availability and prevent abuse ✓ Several controls governed by curated rules are in place to control specific actions on our site like withdrawals and deposits preventing abuse	✓ Betsson has a closed vulnerability disclosure programme where people can report web vulnerabilities on our site ✓ Betsson has a comprehensive Security Incident Management Policy which governs the handling of security incidents following a lifecycle which builds on and follows the NIST (US National Institute of Standards and Technology) Incident Response Plan as part of its CSIRT (Cyber Security Incident Response Team) activities

Information Security Governance

In conclusion, this Policy lays the foundation for the proper governance of information enabling the organisation to meet all gaming regulatory requirements and its obligations when it comes to the handling and protection of information. The framework adopted sets clear expectations on how, amongst others, employees, contractors and third parties shall handle information in a safe and reassuring manner. Ultimate responsibility is carried by Betsson's Operational CEO who delegates the functional responsibility to the Chief Information Security Officer to execute the strategy aimed at protecting value creation as specified in the Policy.