Cyber Security and Data Privacy

Cyber Security

At B.Grimm Power, protecting and monitoring information technology (IT) security are our priorities. Regarding our cyber security governance, the Chief Operating Officer (COO) is accountable for overseen cyber security strategy, which includes setting policies, evaluating, monitoring, to ensure that the IT infrastructure, system, and procedures meet the standards and support the operations. The COO present to the Audit Committee of the Board of Directors every two months. At operational level, the Head of Enterprise Information and Technology (EICT) reports to the COO monthly. The EICT department comprises of 1) Computer Incident Response Division, which responsible for developing a proactive incident response plan, testing, and resolving system vulnerabilities, and providing support for cyber security incident handling, and 2) Information and Communication Technology Division, which responsible for safeguarding IT infrastructure and general IT incident response.

Cyber Security Governance

To ensure effective cyber security management. We have set policies, guidelines, and procedures in place, aligning with the Cybersecurity Framework by the US National Institute of Standards and Technology (NIST) as follows:

Identify	Protect	Detect	Respond	Recover
• IT Asset Management • IT and Business Environment • IT Governance • IT Risk Assessment • IT Risk Management Strategy • Supply Chain Risk Management	• Security Architecture • Identity Management • Access Control • Security Awareness and Training • Data Security • Information Protection Process and Procedure • Preventive Maintenance • Protective technology	• Anomalies and events monitoring process procedure and tools • Anomalies and events detection and analysis • Vulnerability Management • Security Continuous Monitoring	• Cybersecurity Incident Response Planning • Crisis communication (Internal & External) • Cybersecurity incident and event analysis (Investigation) • Impact mitigation	• IT recovery planning processes and procedures to restore systems • Crisis communication (Internal & External) • Implementing improvements based on lessons learned and reviews of existing control

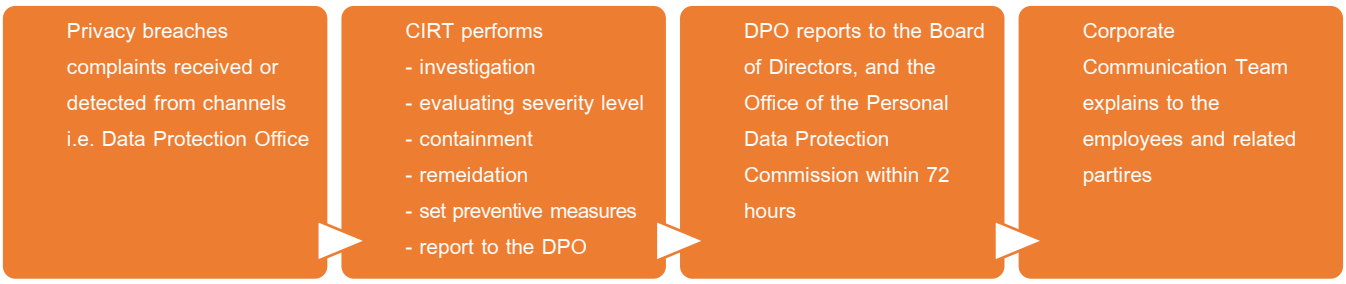
Data Privacy

B.Grimm Power is committed to the protection of all stakeholders' personal data and has appointed the Data Protection Office (DPO) to ensure transparency of data handling practices. The DPO is responsible for setting polices and guidelines to ensure compliance with related regulations, monitoring customer privacy issues, and collaborating with internal business units on privacy protection matters, including handling data breach cases. Aligning with the Personal Data Protection Act. (PDPA), the Privacy Policy has been put in place, describing what personal data we may collect, objectives, customer rights, and contact point. The policy applies to both our own operation and suppliers.

We strive to embed the principles of Privacy by Design and by Default, considering risks and protection related to data privacy, into every stage of new service, software, and system developments. Also, B.Grimm Power has performed a Privacy Impact Assessment (PIA) to identify the risks and impacts to the data privacy, and set out measures to manage and/or mitigate such privacy risks and impacts. The PIA must be integrated into all new application development, software upgrade processes, and any project that will involve the handling of personal information while assessing its compliance with legal obligation i.e., Personal Data Protection Act. In addition, the Internal Audit (IA) unit is responsible for systematic and holistic reviewing and evaluating personal data protection's compliance based on requirements from the Personal Data Protection Act, focusing on activities with risks related to personal data handing, on annual basis, and assisting to guide the company strategy, raising awareness in PDPA compliance through proactive IA audit approach.

We have set the data breach incident response procedures, responding to breaches or leakages related to personal data. In case the customers have any questions or issues can contact the Data Protection Office at dpo@bgrimmpower.com. The escalation process are as follows:

Data Breach Incident Response Process



To build awareness and understanding toward cyber security and data privacy protection, we conduct mandatory trainings on data privacy and cyber security on annual basis, which all employees are required to pass the assessments. A zero-tolerance policy will be applied to non-compliance with cyber security and/or privacy policies, which may result in disciplinary actions and/or legal actions.

Overall, we received no privacy complaints and there were no breaches relating IT security, and infrastructure incident in 2020. For more details about cyber security and data privacy please see Sustainability Report 2020, page 69-71.

Performance Data

	Unit	2018	2019	2020
IT security breaches				
Number of information security breaches or other cybersecurity incidents	Case	0	0	0
Number of data breaches	Case	0	0	0
Number of customers and employees affected by company's data breach	Case	0	0	0
Fines/penalties paid in relation to information security breaches or cybersecurity incident	Baht	0	0	0
IT infrastructure incidents				
Number of IT infrastructure incidents, which resulted in revenue loss or pay penalties	Case	0	0	0
Financial impact from the IT infrastructure incidents	Baht	0	0	0
Substantiated complaints related to breaches of customer privacy				
From individuals and general agencies	Case	0	0	0
From regulatory bodies	Case	0	0	0

We collect the data based on consent or legal requirement. There is no further processing beyond what is covered by the original consent. Following that, no customer data is used for secondary purposes.