B.GRIMM
SINCE 1878

บริษัท บี.กริม เพาเวอร์ จำกัด (มหาชน) สำนักงานใหญ่
B.Grimm Power Public Company Limited (Head Office)
5 ถนนกรุงเทพกรีฑา แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
5 Krungthepkreetha Road, Huamark, Bangkapi, Bangkok 10240
Tel. +66 (0) 2710 3400, Fax +66 (0) 2379 4257
เลขประจำตัวผู้เสียภาษีอากร 0107559000427

Information Technology Security Policy

B.Grimm Power Public Company Limited has established an Information Technology Security Policy, along with related procedures to ensure that its information technology systems are appropriate, efficient, secure, and capable of operating without interruption. These measures aim to prevent potential issues arising from the improper use of information technology systems, as well as to address cyber threats that may impact the organisation's stability. Therefore, B.Grimm Power has implemented an Information Technology Security Policy, setting out standards and procedures for IT system security and appropriate measures to prevent various threats.

Applicability

This policy applies group-wide across B.Grimm Power, covering all employees, operations, subsidiaries, joint ventures and contractors under the organisation's supervision who are authorised to access the company's network systems, computer systems, and all related hardware.

Commitments

- To preserve the confidentiality of critical information, ensure its integrity and accuracy, and maintain its availability so that information can be accessed continuously as authorised, thereby supporting uninterrupted business operations.
- To manage information security in accordance with international standards, with a commitment to continuous improvement and development.
- To ensure that risks and cyber threats to the organisation's information systems are effectively identified, prevented, detected, responded to, and recovered from, thereby minimising potential impacts on B.Grimm Power's operations and business opportunities.
- To support B.Grimm Power's sustainable growth in conducting business in an ever-evolving digital era.

B.Grimm Power has therefore established the following policies to align with these commitments:

1. **Personnel Security Management Policy**

   The People Partnership Department must carry out background checks on job applicants, define employment conditions, and promptly inform the Information Technology Department of any changes in employee status. New employees must undergo training on information systems and data security, and regular training and awareness programmes must be provided for all staff. All employees are required to strictly comply with B.Grimm Power's security policies, legal requirements, and relevant regulations.

บริษัท บี.กริม เพาเวอร์ จำกัด (มหาชน) สำนักงานใหญ่
B.Grimm Power Public Company Limited (Head Office)
5 ถนนกรุงเทพกรีฑา แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
5 Krungthepkreetha Road, Huamark, Bangkapi, Bangkok 10240
Tel. +66 (0) 2710 3400, Fax +66 (0) 2379 4257
เลขประจำตัวผู้เสียภาษีอากร 0107559000427

2. **Physical and Environmental Security Policy**

   B.Grimm Power has established control measures for information technology areas based on their level of criticality, with strict access control for both individuals and equipment. Appropriate protection against physical and environmental threats have been implemented. Furthermore, security incidents must be recorded, monitored, and reported in accordance with defined timelines and procedures.

3. **Access Control Policy**

   B.Grimm Power has established access control measures for data, information systems, and storage devices in accordance with roles and responsibilities. These measures are based on principles of authentication, systematic privilege management, and the use of secure passwords. In addition, remote access, data encryption, and the use of devices are strictly controlled to mitigate risks and ensure data security at all stages.

4. **Network and Server Policy**

   B.Grimm Power has established stringent guidelines for controlling and maintaining the security of its networks. These include access control, monitoring, malware protection, data encryption, encryption key management, security audits, and data backups. These measures aim to prevent threats and effectively respond to unwanted incidents.

5. **Internet Security Policy**

   B.Grimm Power has established clear guidelines for the use of the internet within the organisation to ensure appropriate usage, prevent access to or dissemination of information that could harm B.Grimm Power, and maintain data security. These guidelines include prohibitions on commercial use, the disclosure of confidential information, the responsible use of social media, and the prohibition of inputting data into Generative AI systems without prior authorisation.

6. **Security Development Policy**

   B.Grimm Power has established security practices to ensure that its information systems are continuously improved and maintained to prevent unauthorized access, data leakage, and the development of software that may pose risks. These practices cover access control to source code, separation of development environments, compliance with security standards, and clear prohibitions on developing tools that could adversely affect the system.

7. **Data Breach Policy**

   B.Grimm Power has established management measures to control and restrict access to data, systematically assessing and responding to data leakage incidents. The Cyber Security Department is responsible for monitoring, coordinating, and evaluating risks, as well as recording and maintaining the confidentiality of incidents. Additionally, consideration is given to reporting to external agencies as appropriate.

บริษัท บี.กริม เพาเวอร์ จำกัด (มหาชน) สำนักงานใหญ่
B.Grimm Power Public Company Limited (Head Office)
5 ถนนกรุงเทพกรีฑา แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
5 Krungthepkreetha Road, Huamark, Bangkapi, Bangkok 10240
Tel. +66 (0) 2710 3400, Fax +66 (0) 2379 4257
เลขประจำตัวผู้เสียภาษีอากร 0107559000427

8. **Data Retention and Disposal Policy**

   B.Grimm Power requires that data be securely stored, with controlled access to important or confidential documents and media. It also mandates the proper destruction of data according to its classification and confidentiality level, to prevent unauthorised access and reduce the risk of data breaches.

9. **Data Classification Policy**

   The data classification policy aims to categorise B.Grimm Power's critical information into four levels: public information, internal use information, confidential information, and strictly restricted information. This classification defines the sensitivity and potential impact on financial matters, legal compliance, reputation, and customers clearly, enabling B.Grimm Power to manage data security appropriately and comply with legal requirements effectively.

10. **Incident Response Policy**

    The incident response policy aims to establish a clear process covering preparation, detection, incident management, internal and external communication, as well as continuous evaluation and improvement. It assigns clear roles and responsibilities to users, the information technology department, and relevant units to ensure effective handling of information security incidents in accordance with the organisation's requirements.

11. **Information Security Aspects of Business Continuity Management Policy**

    To ensure the continuity of B.Grimm Power's business operations in the event of unforeseen incidents, the Information Technology department must assess impacts, develop and review the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) at least once a year. These plans should be regularly tested and cover cybersecurity-related incidents. Reports on these activities must be prepared and submitted to senior management to support decision-making.

12. **External Party Relationships Policy**

    B.Grimm Power has established data security requirements in collaboration with external service providers, specifying key issues in the contract, including compliance with the Personal Data Protection Act (PDPA), subcontractor responsibilities, and risk management. B.Grimm Power also regularly monitors, audits, and reviews the services provided under the contract, and any changes must be mutually agreed upon by both parties.

13. **Personal Data Protection Policy**

    B.Grimm Power collects, uses, and discloses personal data in a transparent and fair manner in accordance with the law, based on the data subject's consent or legal exceptions. The data collected includes general information, sensitive data, contact details, financial information, and other relevant data. B.Grimm Power enforces strict data security measures, retains data only for as long as necessary to fulfil the intended purposes, and grants data subjects the right to access, rectify, delete, or object to the use of their data. B.Grimm Power may update this policy from time to time to ensure compliance with applicable laws and evolving best practices.