Energy Absolute group companies

Information Security Policy and Procedure

EA's Information Security Policy and Procedure (the Policy and Procedure) provides comprehensive guidance to Energy Absolute group companies (the Company, EA). Information systems and data are business resources that need effective care and well managed. IT system usage control, access control and system securities control are most important for lowering risk of organization and reducing damage that impact to information systems and data. Energy Absolute group companies have realized the importance of information systems and data protection. We encourage to all employee to have awareness and to be involved in process of protecting information system and data. The policy and procedure applies to executive management and all employees of the Company including the third parties. The policy and procedure's core objectives are followings: (1) to build trust in the company's IT systems among the Board of Directors, (2) to raise security awareness and ensure proper implementation among all employees, (3) to foster knowledge sharing and development for IT personnel through external collaborations, (4) to thoughtfully integrate new technologies, and, (5) to oversee the IT division's operations, ensuring strict adherence to the company's established policies. These aims collectively ensure a secure and reliable IT environment for the company's business operations. The relevant requirements are specified in EA Information Security Policy and Procedure, which has been issued by the IT Department. There are comprised of the followings;

- **Continuously improving Information security** by enhancing its Information security by integrating it into its Business Continuity Plans (BCP). It has defined essential requirements for information security and its continuity during abnormal situations such as crises or disasters. This is achieved through the documentation, implementation, and ongoing maintenance of relevant processes, procedures, and controls to ensure that the required level of information security is maintained even during such adverse events. Additionally, the company conducts annual reviews of its established information security continuity controls to ensure their accuracy, relevance, and effectiveness as followings. Besides, to ensure secure software development and modifications, and to minimize risks that may affect the organization's information systems, change requests must be initiated by authorized personnel and documented in writing, with prior approval obtained from the designated authority before implementation. The deployment of changes into the production environment must be strictly controlled and thoroughly verified. Program information and change history must be accurately and completely recorded, and previous versions must be retained for emergency recovery.

- **Data integrity and protection** by enforcing strict control mechanisms in accordance with clearly defined policies. The objective is to ensure that information technology is used appropriately and securely, while preventing unauthorized access such as from external individuals, computer viruses, or malicious code as well as to protect against potential damage to stored data or system operations. Therefore, it is essential to establish clearly defined operational procedures and responsibilities. The details are as followings;
  - *Incident management procedures*: Define employee responsibilities and establish appropriate response protocols for handling system abnormalities or information security incidents, such as system unresponsiveness, errors from incorrect data entry, leakage of confidential information, or system malfunctions.
  - *Segregation of Duties*: Clearly assign and define responsibilities related to the operation of the company's information systems and networks in order to enhance role clarity and reduce the risk of workplace fraud. This includes separating the duties between system developers and system administrators.
  - *Asset classification and control:* Safeguard information and IT assets by categorizing and managing them appropriately.
  - *Prevention of unauthorized access and data tempering*: Prevent unauthorized access and protect against unauthorized modification of information.
  - *Protection against damage to computer systems*: This includes both physical and environmental security to ensure system availability and resilience.
  - *Access control:* Restrict system and data access only to authorized personnel based on their roles and responsibilities.
  - *Change Control*: Regulate changes and modifications to the company's information systems by documenting all significant changes or edits and notifying relevant stakeholders accordingly.
  - *Protection against malicious software*: Safeguards such as antivirus and anti-malware tools are implemented to prevent threats from harmful software.
  - *Housekeeping and backup management*: Clear procedures are established for regular data backups at least once a year to ensure availability and recoverability.

- **Monitor and Response to information security threats.** The company mandates the immediate reporting of security threats, incidents, and software malfunctions (e.g., computer viruses, security breaches, etc.). System administrators are responsible for documenting all security threats, incidents, and software malfunctions, along with corrective actions taken, to encourage company personnel learning and enhance future response capability development. Management is expected to enforce disciplinary measures for violations of these security policies. Additionally, antivirus and anti-malware solutions have been deployed, supported by continuous system usage monitoring.

- **Responsibility of information security for all individual employees.** The company promotes information security awareness among all employees and defines their responsibilities through the following measures. Establishment of an IT Committee that responsible for monitoring information security practices, guiding IT operations, and advising on policy development. All employees are responsible for complying with information security policy, the mandatory information security training is provided to ensure that all employees understand and adhere to the policy and a formal disciplinary process is enforced in cases of policy violations to ensure accountability. Responsibilities related to information security are clearly defined in employment agreements. Internal Audits are conducted to assess compliance with the policy.

- **Information Security of Third Parties Access Including Suppliers and Service Providers.** The use of information technology services from suppliers and service providers may pose risks to the company, such as access risks and data integrity risks arising from the actions. Therefore, the policy enables the company to utilize such services efficiently, reliably, and to ensure that company's information accessible by suppliers and service providers is adequately protected, the policy and procedures are as followings; ***Establish criteria for selecting*** suppliers and service providers, prioritizing those with a proven track record of reliability and careful operations. ***Information security requirements*** shall be agreed upon and documented of ***Service Level Agreement (SLA)*** with suppliers and service providers that clearly outlines the scope and terms of service, reasons for access, and data confidentiality obligations. The agreement must also specify the provider's rights to access and use the company's systems. Carefully monitor and control suppliers and service providers to ensure their services remain within the agreed scope. This includes assigning company personnel to supervise on-site activities or verify remote operations. In the case of remote access, modems should be disconnected immediately after use. ***Quality control measures*** must also be implemented to maintain the services.

Information Security Management Programs

Energy Absolute group companies have created the Information security policy and procedure to manage Information security and cybersecurity. EA has measures and implement management programs to ensure effective implementation of the policy and procedure are as followings;

- The Company process the Information security related business continuity plans (BCP) testing which involved simulating a scenario where the Cloud system in the company's main data center crashed and recovering from the backup system and operations resumed as planned. The company conducts testing of the Information Technology Disaster Recovery Plan (IT DRP) at least once a year. This plan is designed to prepare for unexpected events or disasters that may impact IT systems and data. Its primary objective is to ensure that critical systems and data can be recovered promptly, enabling business operations to resume with minimal disruption and damage. Test scenarios are selected based on risk assessments related to the systems, and the programs are executed in accordance with the IT Disaster Recovery Plan established by the IT Department.

- Information security vulnerability analysis and external assurance: The company has implemented information security improvements using the Zero Trust approach to elevate data security standards and various company systems by migrating the business group's core systems to Cloud systems that meet international security standards. The company engages service providers for these systems, and external audits of the service providers' systems are conducted annually regarding the information security systems, comply with relevant standards and regulations such as ISO27001, ISO27017, ISO27018, CSA-STAR (Cloud Security Alliance Security, Trust & Assurance Registry), and SOC 2 Type II (System and Organization Controls 2 Type II) to reinforce the trust of stakeholders.

- Internal audits of the company are conducted annually regarding the information technology and information security management systems which including identification of areas requiring improvement (If any), propose audit recommendations to senior management for the actions and follow-up to ensure that identified issues are addresses within a specific timeline.

- Escalation process: In the event of an information security or cybersecurity threats, incidents, and software malfunctions (e.g., computer viruses, security breaches, etc.), employees can inform/ report through IT Management, IT support channels, such as the IT Service Desk (GLPI), to escalate the investigation and resolution.

- Organize training and educated about Information security and policy and procedure to prevent organization risks and employee risks by requiring employees to be aware of and comply with the requirements of information security and cybersecurity, which are enforced and subject to disciplinary actions as specified by the company.

Management Approach

Energy Absolute group companies had set management guidance to manage Information security and cybersecurity Risk by applied international standard NIST Cybersecurity Framework with 5 important procedures.

1. Identify to understand environment, asset and for risk management.
2. Protect system and data by apply standard security protection.
3. Detect threat, monitoring and detection.
4. Response when threat detected for reduce impact and limit system damage.
5. Recover system to normal operation quickly.

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Personal Data Protection & Privacy Procedure

Energy Absolute group companies has created the Personal Data Protection & Privacy Policy (the Policy) to respect the rights to privacy and to ensure that personal data is protected, including the operations, employees, suppliers and stakeholders. The Personal Data Protection & Privacy Policy embedded in group-wide risk management, specifically addressing data privacy risk as part of its business operations. The details are specified in the Policy, which is issued by the IT department. EA has measures and implement procedures to ensure effective implementation of its policy as followings;

- The security of your personal data is treated as important. The Company has implemented appropriate technical and administrative standards to protect your personal data from the loss, misuse, and unauthorized access use, disclose, or destruction. The Company uses technology and security procedures such as encryption and access restriction to ensure that only authorized people will have access to your personal data, and that they are trained about the importance of protecting personal data.

Personal Data Protection & Privacy Procedure (continue)

- The Company provides appropriate security measures to prevent the loss, access, use, change, and disclosure of personal data from those who do not have rights or duties related to that personal data. The Company will review the above-mentioned measures when necessary or when the technology changes to ensure that the security measures are effective.

- Work from anywhere Privacy Policy: The company has devised the work from anywhere scheme to be effective in the event when operations on its premises is untenable and built a mechanism for efficient, unfettered, and secure and rigorously controlled access to its IT system. It has also formulated relevant policies, criteria, and measures to enhance the security of Microsoft Office 365 System, including access management, multi-factor authentication, data access rights and control.

- Personal Data Protection & Privacy Procedures embedded in group-wide risk/compliance management to ensure that all entities within the group operate in accordance with consistent guidelines and standards for the protection of personal data.

- Organize training and educate about Personal data protection & privacy policy/ procedures to all employees and related persons by follow Thailand PDPA Act 2019 by requiring employees to be aware of and comply with the policy/ procedures, which are enforced and subject to disciplinary actions as specified by the company.

- External audits of the service provider's systems are conducted annually regarding compliance with the Personal data protection & privacy policy and procedures.

- Internal audits of the company are conducted annually regarding compliance with the Personal data protection & privacy policy and procedures.

- The company takes strict measures to maintain security as well as preventing uses of your information for other purposes than specified in the company's personal data protection policy without your prior consent.

2024 Performance of EA's Information Security and Personal Data Protection & Privacy

- Percentage of employees attended trainings related to Information security, Cybersecurity and Privacy Data Protection & Privacy.

  2024 : 100%

  2023 : 100%

  2022 : 100%

- Reporting on violations: In 2024, there were no major non-compliances or complaints by any clients, customers and employees on breaches of information security.
  - Number of cyber security breaches 2024 = 0.
  - Number of data breaches 2024 = 0.
  - Number of customer information used for other purposes from consent 2024 = 0.

- Over 90% of employees have the skills, understanding, and ability to use technologies such as Basic AI and various tools in Microsoft Office 365 to effectively and securely to apply, utilize and enhance work efficiency in various functions.

- The Company successfully passed the Business Continuity Plan (BCP) testing which involved simulating a scenario where the Cloud system in the company's main data center crashed and recovering from the backup system and operations resumed as planned, demonstrating the effectiveness of the continuity strategy according to the predetermined plan.

2025 Goals of EA's IT Security and Personal Data Protection & Privacy

- **Strengthen cyber security and personal data protection** by increasing team members for SOC and NOC units and tools to detect and prevent cyber intrusions, including preventing company data leakage.

- **Increase the implementation of artificial intelligence technology** such as Generative AI for use in conjunction with RPA (Robotic Process Automation) to enhance efficiency in internal organizational processes.