Energy Absolute Public Company Limited
89 AIA Capital Center Building, 16th Floor, Ratchadaphisek Road, Dindaeng Sub-District,
Dindaeng District, Bangkok 10400

IT Disaster Recovery Plan

1. Purpose

1.1 To act as a guideline in case of information security emergencies

1.2 To mitigate the impacts or risks that may arise from information security emergencies

2. Scope

This document covers the following aspects: 1) risk assessment of potential incidents related to the IT systems, 2) risk mitigation guidelines, 3) and a risk management plan outlining how to respond to risk incidents that may occur to the information technology systems of Energy Absolute Public Company Limited and all of its subsidiaries, as well as procedures to test the preparedness of the Company's IT Disaster Recovery Plan

3. Reference Documents

None

4. Definition

4.1 IT refers to Information Technology

4.2 The Company refers to Energy Absolute Public Company Limited and all of its subsidiaries

5. Roles & Responsibilities

5.1 The IT Committee is responsible for assessing potential risks that may impact the IT systems and for establishing a set of procedures on mitigating or solving such risks

5.2 IT employees are responsible for preventing, monitoring, and solving such risks as per the procedures or working plans laid out by the IT Committee

6. Procedures

6.1 Risk Assessment

Responsible Person(s)	Details	Related Documents
The IT Committee	The IT Committee should assess risks that may adversely impact the Company's IT systems by categorizing various risks into the following three types: 6.1.1 Human Error Risks 6.1.2 Software Risks 6.1.3 Fire and Electrical Risks	-

6.2 Guidelines on Preparing for Risk Incidents

Responsible Person(s)	Details	Related Documents
The IT Committee	The IT Committee should establish guidelines to mitigate potential risk incidents as follows: 6.2.1 In the case of human error risks, if the department's employee/personnel lack the necessary knowledge or skills regarding both computer hardware and software, which may result in damages, malfunctioning, or disruptions to the Company's IT systems and impede the utilization of said systems at full capacity, the guidelines to mitigate such risks are as follow: • Arrange training modules for the employee to address knowledge or skills gaps regarding the usage and management of both computer hardware and software • Hiring external personnel who possess the knowledge and expertise to supervise, advise, audit, and maintain network systems (both hardware and software) in collaboration with the Company's employees • Defining the clearance level and privileges for each system user in accessing data 6.2.2 In the case of software risks that result in damages to computer equipment or network systems, i.e. a computer infected by a computer virus which disrupts the functioning and damages the Company's IT systems, the guidelines to mitigate such risks are as follow: • Install firewall to protect against external intrusion	-

	• Install antivirus software • Block USB Ports and DVD players for personal computers in the network to prevent access from connecting devices 6.2.3 In the case of fire and electrical risks, such risks should be considered as critical due to the scale of potential damages to the Company’s IT systems, thus they should be prioritized and treated with extreme caution	

6.3 Risk Management Plan

Responsible Person(s)	Details	Related Documents
The IT Department	6.3.1 Level of Severity • Equipment Failure • Data Loss 6.3.2 Risk Management Plan • In the case of equipment failure: a) The IT Department should examine if there are spare parts or not. If they are available, the IT employees should replace damaged equipment with the spare parts b) If there are no spare parts, the IT employees should order new equipment for replacement from a vendor that can deliver the products within two working days • In the case of data loss: a) The IT Department should retrieve backup data that is stored outside of the working area b) The IT Department should contact a contractor or vendor to help with the	-

	system re-installation and restore data within one working day c) The IT Department should inform users to test and verify the functioning of the newly installed system and restored data and report any abnormalities d) In the case that an abnormality or an issue occurs during system testing, the IT Department should perform an analysis to determine the source of the issue and address it accordingly	

6.4 Testing the IT Disaster Recovery Plan

Responsible Person(s)	Details	Related Documents
The IT Department	6.4.1 The IT Department should test the IT Disaster Recovery Plan at least once a year by selecting scenarios for the test simulation according to the risks to the IT systems 6.4.2 Prior to the test simulation, the IT Department should inform pertinent parties in advance via email, including on the following topics: • Date and time of the test simulation • The testing scenario • Potential impacts that may occur to IT system users 6.4.3 When the test simulation is due to occur, the IT Department should perform the tests according to the selected scenarios and proceed with resolving issues and impacts that may arise from the scenarios, as well as preparing a summary report of the testing simulation to inform the IT Committee and to act as a guide for further improvements to the IT systems	-

6.5 Using the Administrator's User Account and Password

Responsible Person(s)	Details	Related Documents
The IT Department	6.5.1 In the case that the administrator's User Account and Password needs to be accessed and used for setting up the systems, the IT Department should contact Vice President of Information Technology and System Development Department 6.5.2 Once the administrator's User Account and Password has been used by the individual of equivalent duties to an administrator and its usage is no longer needed, Vice President of Information Technology and System Development should change the password of the administrator's account.	-

7. Relevant Records

Archived Documents	Storage Location	Duration	Responsible Person(s)
Summary Report of the Testing Simulation	IT Office	5 years	IT Manager