



Information Security Policy

Version 1.0

Document Information

Category	Information
Document	Information Security Policy
Version	1.0
Identifier	AX-PL-004
Status	Approved
Author(s)	
Reviewer(s)	
Approver(s)	
Creation Date	August 20, 2019
Effective Date	August 25, 2019
Control Status	CONTROLLED
Distribution	
Disclaimer	This document contains confidential information. Do not distribute this document without prior approval from the higher management of Ai XPRT.

Document Revision History

Author(s)	Effective Date	Version	Description
Syed Talal Hassan	August 25, 2019	1.0	Created the document

Table of contents

1. Introduction.....	4
2. Objectives	4
3. Scope.....	4
4. Information Security Principles	4
5. Legal & Regulatory Obligations.....	5
6. Suppliers	5
7. Incident Handling.....	5
8. Supporting Policies, Procedures & Guidelines	5
9. Review & Development of Policies	5

1. Introduction

The confidentiality, integrity and availability of all forms of information are critical to the continuous functioning of Ai XPRT. Failure in adequately securing information assets increases the risk of financial and goodwill losses. This information security policy describes how Ai XPRT approaches to information security management. It provides the principle guidelines required to protect Ai XPRT's information systems and assets.

Ai XPRT is committed to secure the data supplied by, generated by and held on behalf of third parties pursuant to the carrying out business activities.

Ai XPRT is committed to a robust implementation of Information Security Management System in accordance with the requirements of information security standard ISO 27001:2013.

2. Objectives

This policy applies to Ai XPRT and its subsidiaries.

The objectives of this policy are to:

1. Provide a framework for establishing a robust information security management system for all Ai XPRT information assets in accordance with ISO 27001:2013.
2. To mitigate the risks associated with the loss, misuse, theft, damage or abuse of Ai XPRT's information assets.
3. Continuous improvement of Information Security Management System through Plan Do Check Act (PDCA) cycle.
4. Ensure that organization as a whole and staff at individual level are aware of and comply with all current applicable laws and regulations.
5. Provide a safe and secure information systems and human resource working environment.
6. Ensure that all staff understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle during the course of business.

3. Scope

This policy applies to all information systems and assets, premises and human resource of Ai XPRT and its subsidiaries.

4. Information Security Principles

Following are the overarching governing principles for the security and management of information at Ai XPRT.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability in accordance with the legislative, regulatory and contractual requirements.
2. All staff covered by the scope of this policy must handle information according to its classification level.
3. Information should be both secure and available to those with a legitimate

- need for access in accordance with its classification level.
4. Breaches of this policy must be reported promptly.

5. Legal & Regulatory Obligations

Ai XPRT is responsible to abide by and comply with all contractual requirements, current applicable laws and regulations.

6. Suppliers

All Ai XPRT's suppliers will comply with Ai XPRT's Suppliers Management Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance while accessing or processing Ai XPRT assets, whether on site or remotely and when subcontracting to other suppliers.

7. Incident Handling

If any staff member of Ai XPRT becomes aware of an information security incident, then they must report it to Information Security Management Representative (ISMR). In case where any information security incident raises a regulatory requirement, Ai XPRT is required to fulfil it.

8. Supporting Policies, Procedures & Guidelines

Ai XPRT has developed supporting policies, procedures and guidelines to strengthen and reinforce this information security policy.

All staff, suppliers and third parties authorised to access Ai XPRT's information assets and/or computing facilities are required to familiarise themselves with these policies to make them compliant with the working environment.

9. Review & Development of Policies

Ai XPRT's information security related policies shall be reviewed by the top management in management review meeting at least once in a year and shall be updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.