



INFORMATION, INFORMATION TECHNOLOGY AND INFORMATION SECURITY POLICIES

AUGUST 2021
VERSION 1.0

ABC MOTORS COMPANY LIMITED
ABC Centre, Military Road, Port Louis

Information Classification: **PUBLIC**



Tables of Contents

Revision History	a
Review and Approval	b
Review Clause.....	b
Update Process	b
Approval Process	b
Availability/ Distribution.....	b
Executive Summary	1
Purpose	1
Scope.....	1
Compliance.....	2
Roles and Responsibilities	2
Policies	3
Password Policy	3
Clean Desk Policy	3
Access Control Policy.....	3
Email Policy	3
Social Media	3
Internet Usage Policy	3
Antivirus Policy	4
Acceptable Use Policy.....	4
Removable Media Policy	4
Incident Response Policy	4
Disaster Recovery Plan	4



Revision History

Version	Date	Author	Comments
1.0	16 August 2021	ABC Motors Company Limited	First release v1.0



Review and Approval

Review Clause

The IT Policy must be reviewed and updated:

- Every year in January,
- As and when changes are deemed necessary to align with business needs.

Update Process

If the document requires updates, then the updates must be made to the document, the version incremented as per below table and the new document will require going through the approval process detailed below before it is made effective.

- Increment of 1.0 for major changes and,
- Increment of 0.1 for minor changes.

Approval Process

The approval process must be in the following order:

1. Approval by Signature from the IT Manager
2. Approval by Signature from Top Management
3. Review and Ratification by Audit and Risk Committee

Availability/ Distribution

Once all approvals have been received, the policy will be published and distributed as may be necessary.



Executive Summary

Purpose

ABC Motors Company Limited (henceforth referred to as "ABC Motors" or the "Company") has issued several IT policies defining access to and usage of the company's computer equipment and IT assets. ABC Motors' IT Policies aim at maintaining and preserving the basic principles of Information, Information Technology, and Information Security. Those basic principles are:

Confidentiality – Only authorized users and processes should be able to access, modify or share data

Integrity – Data should be maintained in a correct state, and it should not be possible to improperly modify it, either accidentally or maliciously.

Availability – Authorized users should be able to access data whenever they need to do so.

ABC Motors' IT Policies also aim at ensuring the smooth and efficient operations of the Company and contribute to the Company's productivity and performance in investment in Technology.

The Company has developed its IT policies based on universally accepted best practices and standards. The IT policies and procedures conform to the two main IT standards namely COBIT and ISO 27002:2013. COBIT is a framework for managing IT risk and was created by Information Systems Audit and Control Association (ISACA).

Management is responsible for the effective implementation of the IT policies and procedures which are overseen by the Audit and Risk Committee. The effectiveness of the policies is also tested during the yearly audit exercise.

Scope

This policy represents ABC Motors position and takes precedence over all other relevant policies which may be developed at individual department level. The policy applies to:

- All Information Technology resources provided by ABC Motors,
- All ABC Motors information systems and network domains,
- All users (including ABC Motors staff, contractors, sub-contractors, and authorized third party commercial service providers) of ABC Motors IT resources.

Compliance to this document is mandatory unless authorized exceptions are obtained (see Exceptions in the Compliance Section).



Compliance

Compliance Measurement

The ABC Motors IT function reserves the right to monitor the use of IT resources and will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tools reports, internal and external audits, and feedback from the policy owner.

Exceptions

Exceptions will be accepted only in exceptional circumstances and after careful consideration. Any exception to the policy must be approved by the IT Manager in advance and must be reported to senior management on a regular basis.

Non-Compliance

Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.

Roles and Responsibilities

The IT Manager is responsible for maintaining the document and providing clarifications pertaining to this document.



Policies

Password Policy

Passwords are an important aspect of computer security. The Password Protection Policy and the Password Construction Guidelines set the standard for password creation, password management, and complexity. The policy also outlines the responsibilities for taking the appropriate steps to select and secure passwords, and applies to all users, including contractors and vendors, with access ABC Motors Systems.

Clean Desk Policy

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an employee's workspace and locked away when the items are not in use, or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. The policy establishes the minimum requirement for maintaining a "clean desk" – where sensitive and critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of sight.

Access Control Policy

ABC Motors is committed to the correct use and management of access controls throughout the organization. Insufficient access controls or unmanaged access to information could lead to the unauthorized disclosure or theft of this information, fraud, and possible litigation. This policy defines the correct use and management of access control within ABC Motors.

Email Policy

ABC Motors provides email services to its employees for business purposes. Email is a powerful tool that can greatly enhance communication when used properly. Any information transmitted or received using our corporate email service should be considered property of ABC Motors.

The purpose of the Email Policy is to detail the company's usage guidelines for its email system and aims to reduce risk of an email-related security incident, foster good business communications both internal and external to the company, and provide for consistent and professional application of the company's email principles.

Social Media

Use of social media by employees, both on a professional and personal level, whether using ABC Motors' property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of ABC Motors' systems to engage in social media is acceptable, provided that, it is done in a professional and responsible manner, does not otherwise violate ABC Motors' policy, is not detrimental to ABC Motors' best interests, and does not interfere with an employee's regular work duties. Social media use from ABC Motors' systems is also subject to monitoring.

Internet Usage Policy

Use of the Internet by employees of ABC Motors is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through ABC Motors is a privilege and all employees must adhere to the policies concerning Internet usage. The Internet Usage Policy details what is deemed appropriate internet browsing behavior and informs employees of their responsibilities and what they should and should not do when internet browsing.



Antivirus Policy

All workstation and server-based assets used for company business, whether connected to the ABC Motors network or as standalone units, must use ABC Motors approved antivirus/antimalware protection software and configuration provided by the ABC Motors IT Department. The policy defines ABC Motors' minimum requirements to address security incidents related to computer viruses and malware.

Acceptable Use Policy

The Acceptable Use Policy outlines the constraints and practices that an ABC Motors employee must agree to for access to the ABC Motors computer equipment and information assets. The acceptable use policy is an integral part of ABC Motors' information security policy. The Company reserves the sole right to change or remove the privileges contained in these policies as it may deem fit.

Removable Media Policy

The Removable Storage Policy aims to reduce the risk of loss or unauthorized exposure of sensitive information maintained by ABC Motors as well as reduce the risk of malware infections on ABC Motors computer equipment.

Incident Response Policy

The incident response policy defines the overall plan for responding to information security incidents at ABC Motors. It defines the characterization of incidents, relationship with other policies and procedures, and reporting requirements. The goal of the Incident Response policy is to provide a framework to ensure that potential information security incidents are managed in an effective and consistent manner. This includes documenting the identification of an incident, immediate response to inform, contain, remediate, and restore service, long term solutions to reduce the chance of recurrence, as well as lessons learnt.

Disaster Recovery Plan

The ABC Motors Disaster Recovery Plan (DRP) documents all the information relevant to the company's ability to withstand a disaster and contains the steps the Division will follow should a disaster occur. The DRP defines the goals and objective for disaster recovery activities as well as roles and responsibilities for the different actors required to effectively recovery from a disaster.