Company IT Policy Handbook *(For Internal Use Only)*

1. Introduction

This IT Policy Handbook outlines the rules, standards, and procedures governing the use of technology resources at ABC Solutions Pte Ltd. The purpose of this document is to ensure that all employees, contractors, and affiliates use company-provided IT systems in a secure, ethical, and efficient manner. These policies are designed to protect both individual users and the company from security threats, data breaches, and misuse of resources. Compliance with this handbook is mandatory, and any violations may result in disciplinary action, including termination of employment and legal proceedings if applicable.

2. Acceptable Use of IT Resources

2.1 General Usage

Employees are granted access to IT resources, including computers, networks, email, and communication platforms, for business-related activities only. Limited personal use is permitted, provided it does not interfere with work duties, consume excessive bandwidth, or breach company security protocols. Activities such as streaming non-work-related media, online gaming, or the use of peer-to-peer file sharing applications are strictly prohibited on company networks.

2.2 Prohibited Activities

Employees must refrain from engaging in activities that could compromise the integrity or reputation of the company. This includes accessing inappropriate or offensive content, engaging in cyberbullying, distributing malicious software, or attempting to bypass company security systems. Employees are also prohibited from using company systems to run private businesses, engage in political campaigning, or participate in unlawful online activities. Violations may result in immediate suspension of IT privileges and disciplinary review.

3. Data Security & Confidentiality

3.1 Data Handling

All company data must be treated as confidential and handled with care. Employees must not download, copy, or transfer sensitive information to personal devices or unauthorized cloud storage platforms. Data must be stored only in approved company systems, and access must be restricted to individuals with legitimate business needs. Employees should immediately report any suspected data leaks, suspicious activity, or loss of data to the IT Security team.

3.2 Password Management

Employees are required to maintain strong, unique passwords for all company accounts. Passwords must contain at least twelve characters, including uppercase letters, lowercase letters, numbers, and special symbols. Sharing of passwords is strictly prohibited. Passwords must be updated at least once every ninety days, and accounts will automatically be locked after five failed login attempts to prevent brute-force attacks.

3.3 Encryption Standards

All sensitive company information must be encrypted both at rest and in transit. Employees are required to use company-approved encryption tools for transmitting confidential files. Emails containing sensitive attachments must be password-protected, and the password must be communicated separately. Unauthorized use of third-party encryption software is not permitted without prior IT department approval.

4. Email & Communication Systems

4.1 Corporate Email

The company's email system is intended for professional communication. Employees must use their corporate email addresses when conducting company business and avoid forwarding sensitive communications to personal accounts. Spam, chain letters, or mass messages unrelated to company business are not allowed. All company emails are considered company property and may be monitored or retrieved by IT when necessary.

4.2 Instant Messaging & Collaboration Tools

Employees may use approved messaging applications, such as corporate chat systems and video conferencing tools, for work-related communication. These platforms must not be used for sharing personal files, conducting private business, or discussing confidential information outside authorized teams. Employees are reminded that all communication on company systems may be logged and audited for compliance purposes.

5. Hardware & Software Usage

5.1 Company Devices

Employees are responsible for the care and proper use of all company-issued devices, including laptops, mobile phones, and peripherals. Devices must not be altered, modified, or used to install unapproved hardware components. Loss, theft, or damage of equipment must be reported immediately to IT so that appropriate security measures can be taken. Employees may be held financially responsible for negligence leading to damage or loss of company property.

5.2 Software Installation

Only software approved and licensed by the IT department may be installed on company systems. Unauthorized downloads or installation of applications, including freeware and shareware, are prohibited as they may contain malware or compromise system security. Employees requiring additional software for work purposes must submit a request to IT, who will evaluate and approve installation based on business need and compliance with licensing agreements.

5.3 Mobile Devices & BYOD (Bring Your Own Device)

Employees who use personal devices for work purposes must comply with company mobile security standards. This includes installing company-approved security applications, enabling password or biometric authentication, and allowing IT to remotely wipe data in the event of device loss or theft. Employees must not store confidential company data permanently on personal devices without encryption and prior approval.

6. Network & Internet Usage

6.1 Network Access

Access to company networks is restricted to authorized users. Employees must connect only through secure, company-approved methods such as VPN connections when working remotely. Unauthorized devices may not be connected to the company's internal network under any circumstances.

6.2 Internet Usage

The company provides internet access for professional use. Employees are expected to avoid excessive browsing of non-work-related websites and must not access sites containing adult content, gambling services, or illegal material. Internet activity may be monitored to ensure compliance with security and usage policies. Employees found engaging in inappropriate online activities may face disciplinary action.

7. Cybersecurity & Incident Response

7.1 Employee Responsibilities

Cybersecurity is a shared responsibility. Employees must remain vigilant against phishing attempts, suspicious links, and unexpected email attachments. All employees are required to complete mandatory cybersecurity awareness training annually. Any suspected security incidents must be reported immediately to the IT Security team.

7.2 Incident Response

In the event of a security breach, the IT department will initiate the company's Incident Response Plan. Employees may be required to cooperate by providing logs, system access, or statements regarding their activities. Prompt reporting and collaboration are critical to minimizing potential damage. Employees who fail to report incidents in a timely manner may face disciplinary measures.

8. Remote Work IT Guidelines

Employees working remotely must ensure that they use secure, private internet connections. Public Wi-Fi networks should be avoided unless connected through a company VPN. Remote workers are required to keep devices updated with the latest security patches, antivirus software, and operating system upgrades. Company documents must not be printed or stored in unsecured home environments where unauthorized individuals may gain access.

9. Policy Compliance & Enforcement

Compliance with this IT Policy is mandatory for all employees, contractors, and third-party partners with access to company systems. Failure to comply may result in disciplinary action, up to and including termination of employment. In cases involving breaches of data privacy laws or cybersecurity regulations, employees may also face legal penalties. The IT department reserves the right to monitor, audit, and review system usage at any time to ensure compliance.

10. Policy Review

This IT Policy will be reviewed on an annual basis by the IT department in coordination with HR and senior management. Updates may be issued at any time to reflect new technologies, regulatory requirements, or emerging cybersecurity threats. Employees are responsible for staying informed about policy changes communicated through official company channels.