Revised for

2025

I.T POLICY MANUAL 1.0

This IT Policy manual is designed by Origin 365 following standard norms and compliances. It has been designed to help everyone and every Small and Medium size business set the right policies to govern users and their IT infrastructure. Modification is allowed to suit your needs. Download and Adapt to your environment. If you wish for a customized one adapted to your environment please reach out immediately, we are here to guide you all the way

IT POLICY MANUAL

Version: 1.0
Effective Date: 01-01-2025
Approved By: Origin 365 & Daddy Vice

1. Introduction

1.1 Purpose

The purpose of this IT Policy Manual is to establish a framework for managing and safeguarding the organization's information technology (IT) systems. This document outlines policies that ensure the security, integrity, and efficiency of IT resources while complying with international standards and regulations.

1.2 Scope

This IT Policy Manual applies to all employees, interns, contractors, vendors, and third parties who access, use, or manage the organization's IT systems, networks, and data.

1.3 Audience

This document is intended for IT personnel, management, employees, and any individuals with access to the organization's IT resources.

2. Acceptable Use Policy

2.1 General Use

IT resources must be used solely for business-related activities. Personal use of IT resources should be minimal and must not interfere with business operations. Unauthorized software installations and modifications to IT systems are strictly prohibited.

Users are not to bring other apparels to work aside the ones issued by the organization. Items like switches, repeaters, personal laptops are not allowed. Only phones and tablets are permitted.

Users are not allowed to plug in peripheral devices such as USB, External hard drives or phones to systems. Request permission from the IT department before using any of such.

2.2 Email and Internet Usage

Employees must not use organizational email for personal or unauthorized business communications.
Internet usage should be aligned with professional and ethical standards.
Access to illegal or inappropriate websites is strictly prohibited.

2.3 Mobile Devices & Remote Access

All mobile devices accessing company data must comply with security standards.
Remote access is only permitted through secure and approved methods, such as VPN and multi-factor authentication (MFA).

3. Data Protection & Privacy Policy

3.1 Data Classification

Data is classified as Public, Internal, Confidential, and Restricted.
Sensitive data handling must adhere to regulatory requirements such as GDPR, ISO 27001, and other applicable data protection laws.

3.2 Data Storage & Retention

Data must be stored securely on authorized storage solutions.
Retention policies must be followed, and obsolete data must be disposed of securely.

3.3 Personal Data Protection

Personally Identifiable Information (PII) must be handled with confidentiality.
Encryption and access controls must be in place for PII storage and transmission.

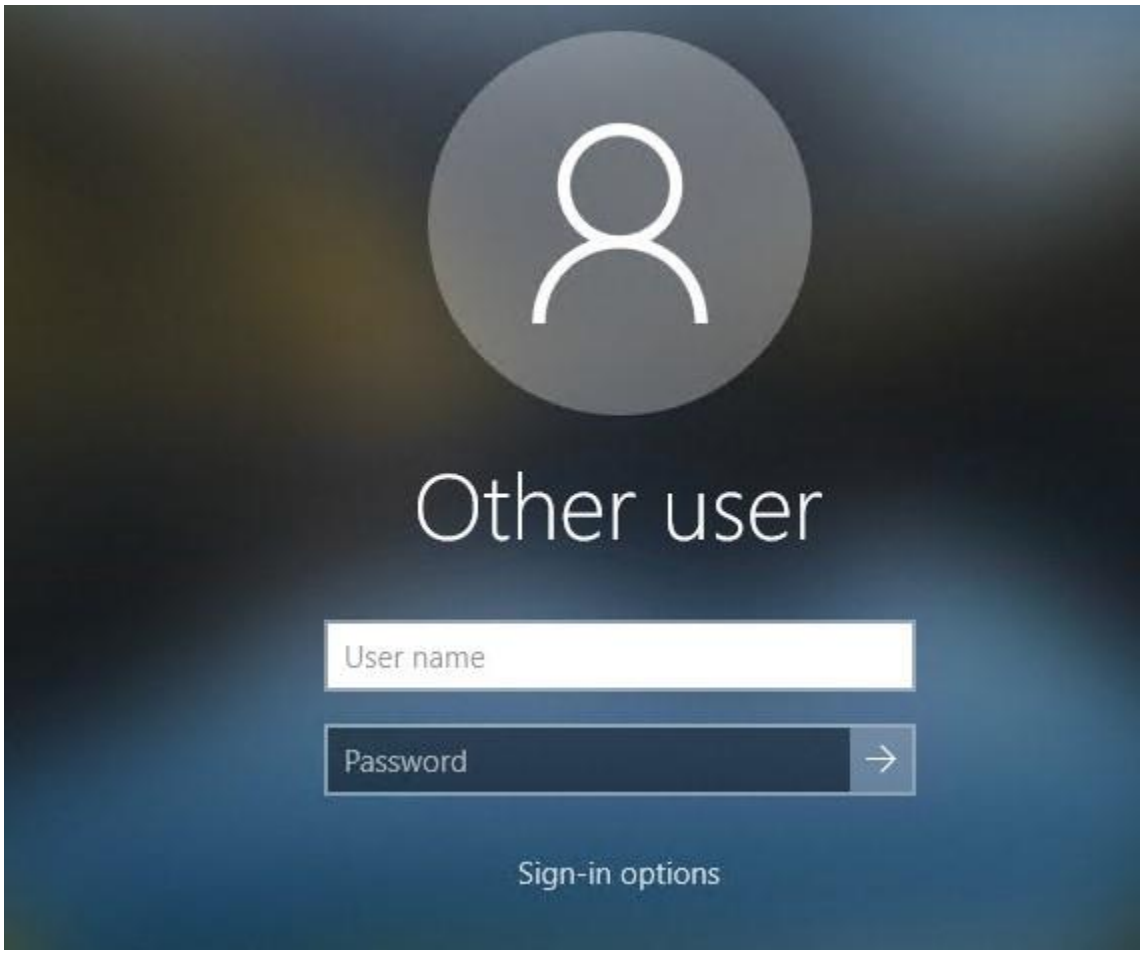
4. IT Security Policy

4.1 Access Control

Role-based access control (RBAC) must be implemented.
Default accounts and passwords must be changed before deployment.
Multi-factor authentication (MFA) must be enforced where applicable.

4.2 User Credentials

During onboarding, every user is presented with user account or login credentials in order to access systems and resources. The credentials include a user name and password.



In case you forget your password or suspect your system has been compromised or Account locked. Please report immediately to the IT department.

4.3 Network Security

Firewalls and intrusion detection systems (IDS) must be deployed. Regular vulnerability assessments and penetration testing must be conducted.

To access wireless connections, every user must request access from the IT department. Users will be presented with credentials to access the WLAN upon the presentation of the device to the IT department.

Note that: it must be a registered device in the IT Directory.

4.4 Endpoint Security

Anti-virus and endpoint protection software must be installed on all devices.
Unauthorized devices must not be connected to corporate networks.

5. Incident Response & Management Policy

5.1 Incident Reporting

All security incidents must be reported immediately to the IT Security Team.
Employees must be trained on identifying and responding to security threats.

5.2 Incident Containment & Resolution

Security incidents must be investigated and documented.
Affected systems must be isolated to prevent further compromise.
Corrective and preventive measures must be implemented.

5.3 Business Continuity & Disaster Recovery

Regular backups of critical data must be performed.
Disaster recovery plans must be tested periodically.

6. Compliance & Legal Framework

6.1 Regulatory Compliance

The organization must comply with international standards such as ISO 27001, GDPR, NIST, and other relevant frameworks.
Employees must be aware of legal obligations regarding IT security and data protection.

6.2 Policy Enforcement

Non-compliance with IT policies may result in disciplinary action, including termination.
Regular audits must be conducted to ensure adherence to policies.

7. Policy Review & Updates

This IT Policy Manual will be reviewed annually or as necessary.
Updates will be communicated to all stakeholders promptly.

8. Best Security Practices to Reduce the Risk of a Security Breach in a Company

In today's digital age, businesses face increasing threats from cybercriminals, making security a top priority. A security breach can lead to financial losses, reputational damage, and legal consequences. Implementing strong security practices is essential to protect company assets, customer data, and business operations. Below are the best security measures that can significantly reduce the risk of a security breach in any organization.

1. Implement Strong Access Control Measures

Limiting access to sensitive systems and data is crucial for preventing unauthorized access.

✓ **Use Multi-Factor Authentication (MFA):** Require employees to verify their identity through multiple methods, such as passwords and biometric scans.
✓ **Enforce the Principle of Least Privilege (PoLP):** Only provide employees access to the data and systems necessary for their job and nothing else.
✓ **Regularly Review and Update Permissions:** Ensure former employees or inactive accounts are deactivated promptly.

2. Regularly Update and Patch Systems

Outdated software and systems are common targets for hackers. Keeping systems updated minimizes vulnerabilities.

✓ **Enable Automatic Updates:** Ensure all operating systems, software, and security tools receive regular updates.
✓ **Patch Known Vulnerabilities:** Regularly apply security patches to fix weaknesses before cybercriminals exploit them.
✓ **Use Endpoint Detection and Response (EDR) Tools:** These tools provide advanced security monitoring for devices connected to the company network.

3. Strengthen Network Security

A secure network prevents unauthorized users from gaining access to company resources.

✓ **Use Firewalls:** Set up firewalls to monitor and block suspicious traffic.
✓ **Encrypt Data in Transit and at Rest:** Use encryption protocols like TLS/SSL for data transfers and AES-256 for stored data.
✓ **Segment the Network:** Separate critical systems from general employee networks to limit access.
✓ **Monitor Network Traffic:** Use Intrusion Detection Systems (IDS) to identify suspicious activities in real time.

4. Train Employees on Cybersecurity Awareness

Human error is a leading cause of security breaches. Educating employees on cybersecurity best practices can prevent attacks.

✓ **Conduct Regular Security Training:** Teach employees how to recognize phishing emails, malware, and social engineering attacks.
✓ **Implement a Strong Password Policy:** Require complex passwords and regular password changes.
✓ **Simulate Phishing Attacks:** Test employees with fake phishing emails to assess their response and awareness.

5. Implement Secure Data Management Practices

Data protection is essential for compliance and security.

✓ **Back up Data Regularly:** Store backups in secure, offsite locations to prevent data loss due to ransomware attacks.
✓ **Use Data Loss Prevention (DLP) Tools:** Monitor and control data transfers to prevent leaks.
✓ **Limit USB and External Device Usage:** Restrict the use of unauthorized external storage devices to avoid data theft

6. Monitor and Respond to Threats in Real-Time

Early detection of cyber threats helps mitigate risks before they cause major damage.

✓ **Use Security Information and Event Management (SIEM) Systems:** These tools provide real-time threat analysis and reporting.
✓ **set up Incident Response Plans:** Establish protocols for handling security breaches, including containment, investigation, and recovery.
✓ **Conduct Regular Security Audits:** Test security measures through vulnerability assessments and penetration testing.

7. Secure Cloud Services and Remote Work Environments

With remote work and cloud adoption increasing, securing these environments is essential.

✓ **Use Secure VPNs:** Encrypt internet connections for remote employees.
✓ **Implement Cloud Security Controls:** Enable role-based access, logging, and encryption for cloud applications.

✓ **Monitor Remote Devices:** Ensure all employee devices comply with security policies before accessing company networks.

8. Comply with Security Regulations and Industry Standards

Following compliance requirements enhances security and builds customer trust.

✓ **Adhere to GDPR, HIPAA, or ISO 27001 (Depending on Industry):** Ensure data protection policies align with industry regulations.

✓ **Implement Zero Trust Architecture:** Assume no one is automatically trusted, and continuously verify access requests.

✓ **Regularly Review Security Policies:** Keep security guidelines up to date with emerging threats.

N.B: Keep in mind, No security system is 100% foolproof, but implementing these best practices can greatly reduce the risk of a security breach. Companies must continuously update security measures, train employees, and stay vigilant against evolving threats. A proactive approach to cybersecurity not only protects company assets but also ensures business continuity and customer trust.