Revised for 2025

# Cybersecurity POLICY MANUAL 1.0

This IT Cybersecurity Policy manual is designed by Origin 365 following standard norms and compliances. The guide has been designed to help everyone and every Small and Medium size business set the right measures to tackle disaster recovery in case of breach. 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 CYBERSECURITY POLICY MANUAL

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

## 1. Disaster Recovery Plan

### 1.1 Purpose

This Disaster Recovery Plan (DRP) outlines procedures to restore IT systems and data in the event of failures, cyberattacks, or disasters.

### 1.2 Scope

This plan applies to all IT infrastructure, networks, software, and cloud services used within the company.

### 1.3 Key Steps

1. Risk Assessment: Identify critical assets and potential threats.
2. Backup Strategy: Maintain regular backups of essential data and systems.
3. Recovery Process:
   - Restore systems from backup images.
   - Reconnect network components and test functionality.
4. Communication Plan: Notify stakeholders, employees, and relevant authorities.
5. Testing & Updates: Conduct regular drills to validate recovery procedures.

## 2. Acceptable Use Policy (AUP)

### 2.1 Purpose

The AUP establishes rules for employees regarding the use of company IT resources to ensure security and efficiency.

### 2.2 Scope

This policy applies to all employees, contractors, and third parties with access to company IT resources.

### 2.3 Guidelines

1. Prohibited Activities:
   - Unauthorized access to systems.
   - Sharing login credentials.
   - Downloading unapproved software.
2. Email & Internet Usage:
   - Use corporate email for business purposes only.
   - Avoid visiting malicious or unauthorized websites.
3. Data Security:
   - Do not share sensitive company information externally.
   - Report security incidents immediately.

## 3. Incident Response Plan

### 3.1 Purpose

This plan defines how the company will respond to cybersecurity incidents to minimize damage and recovery time.

### 3.2 Scope

This policy applies to all types of security incidents, including malware attacks, data breaches, and system intrusions.

### 3.3 Response Procedure

1. Identification:
   - Detect and confirm the security incident.
   - Assess the impact.
2. Containment:
   - Isolate affected systems.
   - Disable compromised accounts.
3. Eradication:
   - Remove malware or threats.
   - Apply patches and security fixes.
4. Recovery:
   - Restore systems from secure backups.
   - Monitor for reoccurrence.
5. Post-Incident Review:

- Analyze the incident and improve security measures.
- Document lessons learned.

## 4. Data Backup & Retention Policy

### 4.1 Purpose

This policy defines how company data is backed up, stored, and retained to ensure business continuity and regulatory compliance.

### 4.2 Scope

Applies to all digital records, databases, and business-critical information stored on company systems or cloud services.

### 4.3 Backup Strategy

1. Backup Frequency:
   - Daily incremental backups.
   - Weekly full backups.
2. Storage Locations:
   - Secure on-premise servers.
   - Cloud-based backup solutions.
3. Retention Periods:
   - Operational data: 1 year.
   - Financial records: 5 years.
   - Compliance-related records: As per legal requirements.
4. Testing & Monitoring:
   - Conduct regular tests to verify backup integrity.
   - Monitor backup logs for errors.

### Approval & Review

This IT and Cybersecurity Policy Manual shall be reviewed annually or as needed to address emerging threats and compliance requirements.

**Authorized By:**
[Name]
[Title]
[Date]

## 5. 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.