CRCYBER

Cybersecurity Policies and Procedures for SMBs

A practical guide to safeguarding your business with essential cybersecurity policies and procedures tailored for Small Medium Businesses (SMBs).

Cybersecurity Policies & Procedures for SMBs

Cyberattacks on Small Medium Businesses (SMBs) are rising, with hackers targeting businesses that lack strong defences. A single breach can compromise sensitive data, disrupt operations, cause severe financial and reputational harm.

This guide offers clear, practical cybersecurity policies and procedures to help SMBs protect their business and stay resilient against evolving threats.

Recognising and Mitigating Cybersecurity Risks

- **Common cyber threats**: Ransomware, phishing, and insider threats targeting SMBs.
- **Impact of cyber incidents**: Financial losses, reputational damage, and legal consequences.
- **Proactive cybersecurity measures**: Implementing security policies, employee training, and technology solutions.
- **Scam Messages**: Cybercriminals impersonate trusted individuals to trick businesses into sending money or disclosing sensitive information.

CRCYBER Tips:

- Schedule regular security audits to detect weaknesses before cybercriminals do.
- Use email filtering tools to detect and block scam messages.

Crafting an Effective Cybersecurity Policy

- **Why SMBs need a policy**: Establish clear security standards and accountability.
- **Key components**: Risk assessments, data handling, employee guidelines, and compliance.
- **Aligning with business needs:** Customising security measures based on company size and industry.
- **Legal risks:** Non-compliance can result in fines, lawsuits, and reputational damage.

CRCYBER Tips:

- Regularly review and update policies based on emerging threats.
- Assign a cybersecurity champion within your team to drive policy implementation and enforcement.

Access Control and Authentication

- **Strong password policies**: Require rotating complex passwords or passphrases.
- **Multi-factor authentication (MFA)**: Adds an extra layer of security to user accounts.
- **Role-based access control (RBAC)**: Restricts access to sensitive data based on job roles.
- **Password managers**: Reduce security risks by securely storing credentials with a master password.

CRCYBER Tip:

- Regularly review and revoke access permissions for former employees and stale accounts.

Data Protection and Privacy

- **Data classification:** Identify and secure sensitive business data.
- **Encryption:** Protects data during storage and transmission.
- **Secure storage & disposal:** Ensure proper handling of digital and physical records.
- **Compliance laws:** Australian Privacy Act / Notifiable Data Breaches (NDB) scheme, and Payment Card Industry Data Security Standard (PCI-DSS).

CRCYBER Tip:

- **Backup strategies:** Adhere to 3,2,1 backup rule to protect against loss of data.

Network and Endpoint Security

- **Essential tools:** Firewalls, Intrusion Detection Systems (IDS), and antivirus software.
- **Securing networks:** Use strong Wi-Fi encryption and limit remote access.
- **Protecting devices:** Install endpoint protection for laptops, phones, and Internet of Things (IoT) devices.
- **VPNs for remote work:** Secure access for employees working outside the office.

CRCYBER Tip:

- Implement eXtended Detection and Response (XDR).
- Set up alerts for suspicious login attempts to detect unauthorised access early.

Employee Training and Awareness

- **Employees as the first line of defence:** Reducing human error in cyber incidents.
- **Cybersecurity training:** Implement periodic phishing simulations to test and improve awareness.
- **Recognising scams:** Teach staff how to identify suspicious emails and links.

CRCYBER Tip:

- Establish a clear process for reporting security incidents.

Building a Resilient Incident Response and Recovery Strategy

Business Continuity and Disaster Recovery (BCDR) Plan

- **Recovery strategies**: Backup data and establish alternative communication channels.
- **Preventative measures**: Use redundancies to reduce downtime.
- **Testing & drills**: Simulate cyber incidents for preparedness.
- **Ongoing improvements**: Update the plan based on past incidents.

Incident Response (IR) Plan

- **Documented response plan:** Outline steps to identify, protect, detect, respond and recover any incidents.
- **Incident severity levels:** Categorise threats for a prioritised response.
- **Dedicated response team:** Assign IT leads, forensic analysts, and communication officers.
- **Post-incident review:** Analyse breaches to prevent future attacks.

Reporting Cyber Incidents to the ACSC

- **Know reporting requirements:** Some sectors must report to the Australian Cyber Security Centre (ACSC), as required under the Australian Government's Cyber Incident Reporting requirements.
- **Define reporting steps:** Establish an internal process for incident disclosures.
- **Maintain records:** Keep documentation of cyber incidents and responses.
- **Legal consultation:** Understand privacy laws before reporting breaches.

Call to Action

Cybersecurity is an ongoing process that requires vigilance and adaptation. By implementing these policies and procedures, SMBs can protect their data, maintain business continuity, and avoid costly cyber incidents.

As threats continue to evolve, staying proactive is key. Regular training, policy updates, and investment in security technologies will help safeguard your business.

Need expert guidance? Contact us today to strengthen your cybersecurity strategy and protect your business from cyber threats!

CRCYBER

At CRCYBER we specialise in enhancing cybersecurity maturity through Tier 1 managed services with a strong security focus. Our expertise includes professional IT infrastructure services and seamless hardware procurement solutions.

“GOOD PEOPLE,

GOOD SERVICE,

GOOD OUTCOMES.”

Enquire Today
contact@crcyber.com
www.CRCYBER.com

Authored By Eryn Norie & Ged Grimwade
February 2025