Logical Solutions ICT Cyber Security Policy Service

Logical Solutions has been involved in cyber security for many years. It is becoming increasingly crucial that formal policies are implemented that detail security and the best practices surrounding an organisation's ICT platform.

Why do we need a Cyber Security Policy?
A security policy is essential for any organisation using digital devices to store or transmit sensitive information electronically.

- Protecting Sensitive data
- Providing some form of Structured Email Security
- Compliance with Regulations
- Minimises the risk of Cyber Attack
- Mitigates most legal liabilities.

An ICT security policy is vital to any organisation's cybersecurity strategy. It helps to protect sensitive information, comply with regulations, minimise the risk of cyber-attacks, and mitigate legal liabilities.

What problems does having a Cyber Security Policy solve?
A cybersecurity policy can solve several security problems organisations face regarding information and communication technology (ICT).

Overall, a cybersecurity policy can help address several problems related to ICT security, including lack of awareness, inconsistent security practices, vulnerabilities in software and systems, lack of a response plan, and compliance issues. Implementing a comprehensive cybersecurity policy can reduce cyber-attack risk and protect sensitive information.

What are the risks of not having a Cyber Security Policy?
Not having a cybersecurity policy can expose you to various risks, including:

1. Data Breaches: Without a cybersecurity policy, sensitive data, such as customer information, financial records, and intellectual property, can be vulnerable to cyber-attacks. Data breaches can result in significant financial losses, legal liabilities, and reputational damage.

2. Malware Attacks: Malware, including viruses, worms, and Trojan horses, can infect your computer systems and compromise security. A cybersecurity policy can help prevent malware attacks by outlining procedures for keeping software updated and implementing security measures like firewalls and antivirus software.

3. Phishing Scams: Phishing scams are a common way for cybercriminals to steal sensitive information by tricking users into providing personal or financial information. A cybersecurity policy can help educate employees on identifying and avoiding phishing scams.

4. Employee Negligence: Employees may inadvertently expose your sensitive information through their actions, such as using weak passwords or clicking on

suspicious links. A cybersecurity policy can establish guidelines for employee behaviour, including password management, email usage, and acceptable use of company devices.

5. Regulatory Compliance: Many industries are subject to regulations governing the protection of sensitive data, such as healthcare and financial services. Not having a cybersecurity policy can put you at risk of non-compliance, resulting in legal and economic consequences.

A comprehensive cybersecurity policy can help mitigate these risks and protect your valuable data and assets from cyber threats.

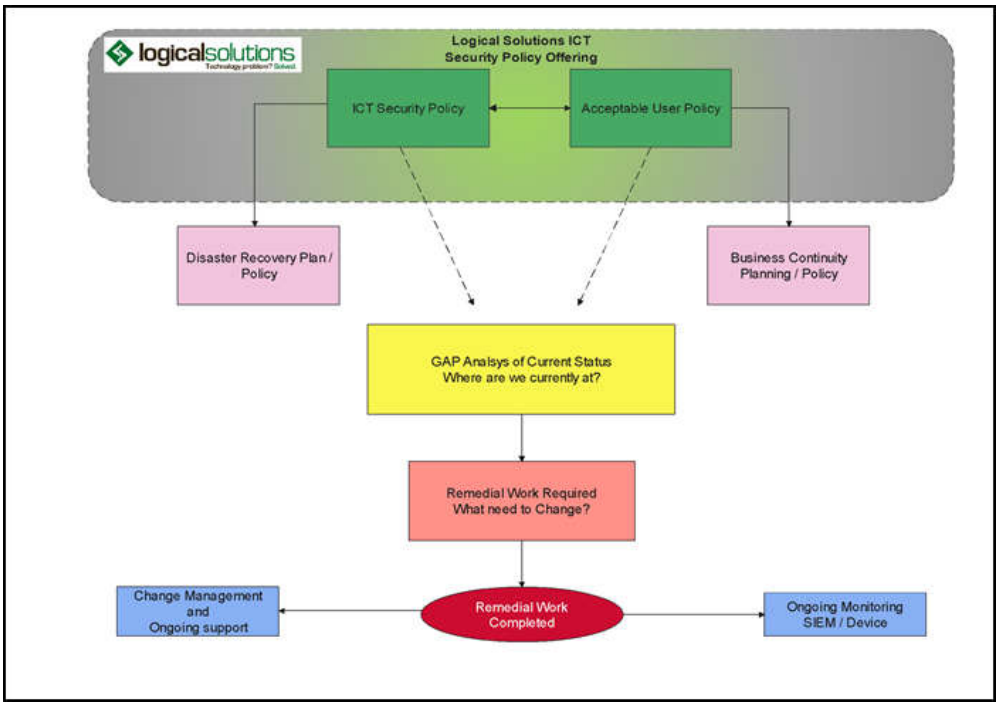
What is the difference between the Zero Trust Framework and a Cyber Security Policy?

A cybersecurity policy outlines an organisation's overall approach to cybersecurity, while zero trust is a security model that can be implemented as part of a broader cybersecurity strategy. A cybersecurity policy may include guidelines for implementing a zero-trust model, but zero trust is not the same as a cybersecurity policy.

The Zero Trust framework aims to provide a more comprehensive and proactive security approach compared to traditional perimeter-based security models, which assume that anything inside the network is already trusted and is used in conjunction with your cyber security policy.

What is included in a Logical Solutions Cyber Security Policy?

The Logical Solutions offering includes the ICT security policy and an acceptable use policy (often included in an employee's employment contract). As you can see below, other policies may be required to satisfy the policy's requirements thoroughly. They are available via optional further engagements.



Security policy sections:

1. Purpose and Scope: This section defines the purpose and scope of the policy, including the objectives of the policy, the types of ICT resources that are covered, and the employees and contractors who are subject to the policy.

2. Roles and Responsibilities: This section outlines the roles and responsibilities of employees, contractors, and third-party vendors concerning ICT security, including their responsibility to report security incidents and comply with the policy.

3. Access Control: This section outlines the procedures for managing user access to ICT resources, including user authentication, password management, and access rights.

4. Data Protection: This section defines procedures for protecting sensitive data, including data encryption, data backup and recovery, and data retention policies.

5. Network Security: This section defines procedures for securing the organisation's network infrastructure, including firewalls, intrusion detection and prevention, and network segmentation.

6. Incident Response and Reporting: This section outlines procedures for responding to security incidents, including incident reporting, investigation, and containment.

7. Business Continuity: This section defines procedures for ensuring the continuity of business operations in the event of a security incident or disaster, including disaster recovery and contingency planning.

8. Training and Awareness: This section outlines procedures for training employees and contractors on ICT security awareness, including phishing and social engineering, safe browsing, and email practices.

Deliverables

A cybersecurity policy can help establish a comprehensive approach to managing cybersecurity risks. Overall, having a cybersecurity policy helps establish a culture of security within and ensures that cybersecurity risks are managed consistently and systematically.

The deliverable at the end of this engagement is to produce an ICT security policy folder which will include an "Acceptable user policy" that can be added to your user's employment contracts. These documents, where possible, will be customised to your organisation without impacting the strength of the overall policy.

The policies will be delivered in PDF format and a physical printed copy within a folder.