Cyber Governance

- ✓ This discussion is about the practical. No Pie in the Sky theories
- ✓ This will not be technical.
- ✓ No Products or Services. Just Information.

Cyber Goverance for Small, Medium, Business

Corporate Governance

INFORMATION SECURITY POLICY

- We all have one.
- Is it High Level?
- Has it been updated?
- Has it been tested?

Cyber Security Policy

FOCUS ON WHAT IS MOST IMPORTANT?

Real Assets, not just IT.

Is it part of Business Continuity Plan?

Is it properly funded?

Real World

NO ONE IS IMMUNE.

No network is secure.
It's a matter of time.

Security must be layered, monitored, updated.

Incident Response Team must be capable and ready..

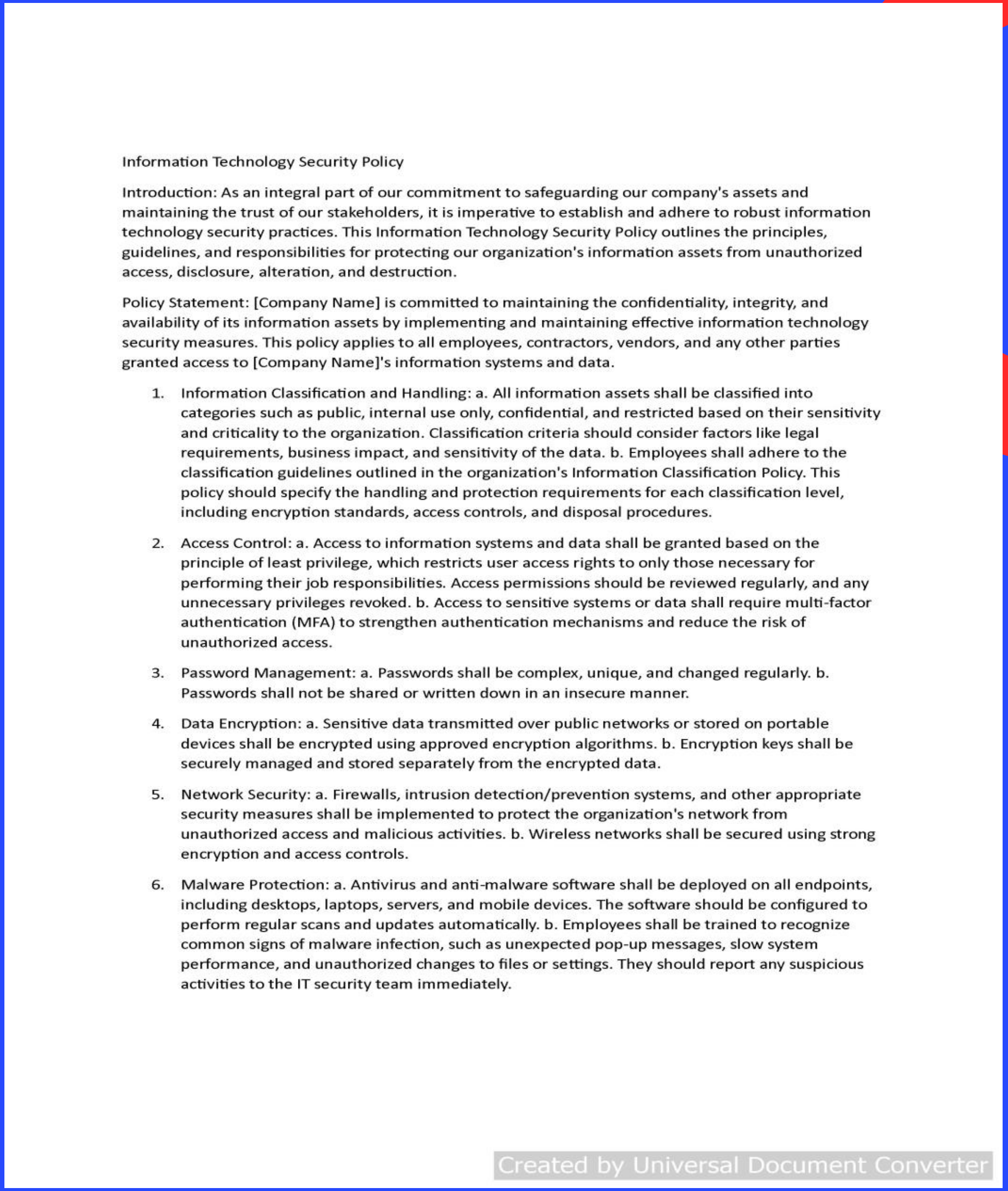
Corporate Governance

- **Information Security is a Business Issue.**
- **Not to be delegated to IT.**
- **Requires C level Participation.**
- **Focus on Real Assets of the Company.**
- Includes:
  - **Information Technology Security Policy**
  - **Cybersecurity Policy**
  - **Business Continuity and Disaster Recovery**

Information Technology Security Policy

Typical Information Security Policy.

- High Level Policy Statement.
- Signed by the CISO and CEO.
- Approved by Board of Directors.
- Employees to sign an Acknowledgement Form.
- Reviewed and Updated Annually,



Information Technology Security Policy

Introduction: As an integral part of our commitment to safeguarding our company's assets and maintaining the trust of our stakeholders, it is imperative to establish and adhere to robust information technology security practices. This Information Technology Security Policy outlines the principles, guidelines, and responsibilities for protecting our organization's information assets from unauthorized access, disclosure, alteration, and destruction.

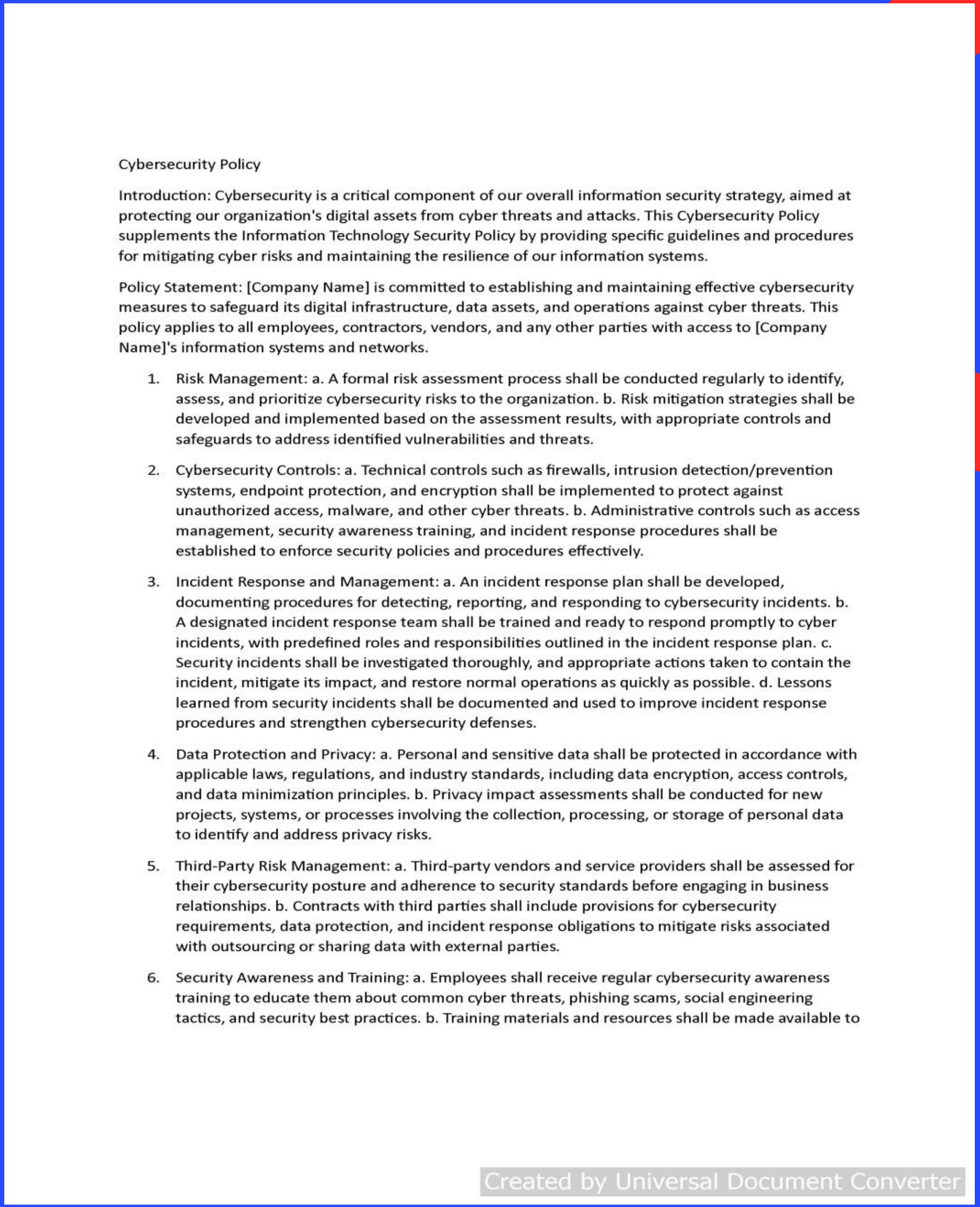
Policy Statement: [Company Name] is committed to maintaining the confidentiality, integrity, and availability of its information assets by implementing and maintaining effective information technology security measures. This policy applies to all employees, contractors, vendors, and any other parties granted access to [Company Name]'s information systems and data.

1. Information Classification and Handling: a. All information assets shall be classified into categories such as public, internal use only, confidential, and restricted based on their sensitivity and criticality to the organization. Classification criteria should consider factors like legal requirements, business impact, and sensitivity of the data. b. Employees shall adhere to the classification guidelines outlined in the organization's Information Classification Policy. This policy should specify the handling and protection requirements for each classification level, including encryption standards, access controls, and disposal procedures.
2. Access Control: a. Access to information systems and data shall be granted based on the principle of least privilege, which restricts user access rights to only those necessary for performing their job responsibilities. Access permissions should be reviewed regularly, and any unnecessary privileges revoked. b. Access to sensitive systems or data shall require multi-factor authentication (MFA) to strengthen authentication mechanisms and reduce the risk of unauthorized access.
3. Password Management: a. Passwords shall be complex, unique, and changed regularly. b. Passwords shall not be shared or written down in an insecure manner.
4. Data Encryption: a. Sensitive data transmitted over public networks or stored on portable devices shall be encrypted using approved encryption algorithms. b. Encryption keys shall be securely managed and stored separately from the encrypted data.
5. Network Security: a. Firewalls, intrusion detection/prevention systems, and other appropriate security measures shall be implemented to protect the organization's network from unauthorized access and malicious activities. b. Wireless networks shall be secured using strong encryption and access controls.
6. Malware Protection: a. Antivirus and anti-malware software shall be deployed on all endpoints, including desktops, laptops, servers, and mobile devices. The software should be configured to perform regular scans and updates automatically. b. Employees shall be trained to recognize common signs of malware infection, such as unexpected pop-up messages, slow system performance, and unauthorized changes to files or settings. They should report any suspicious activities to the IT security team immediately.

Cybersecurity Policy

Typic**al High Level Policy.**

- General description of cybersecurity controls.
- Requires development of Incident Response Plan to Detect, Report, and Respond.
- Designated Incident Response Team trained and ready to respond.
- Requires Employee Training.
- Lessons Learned and Continuous Improvement.
- **No Details.**



Cybersecurity Policy

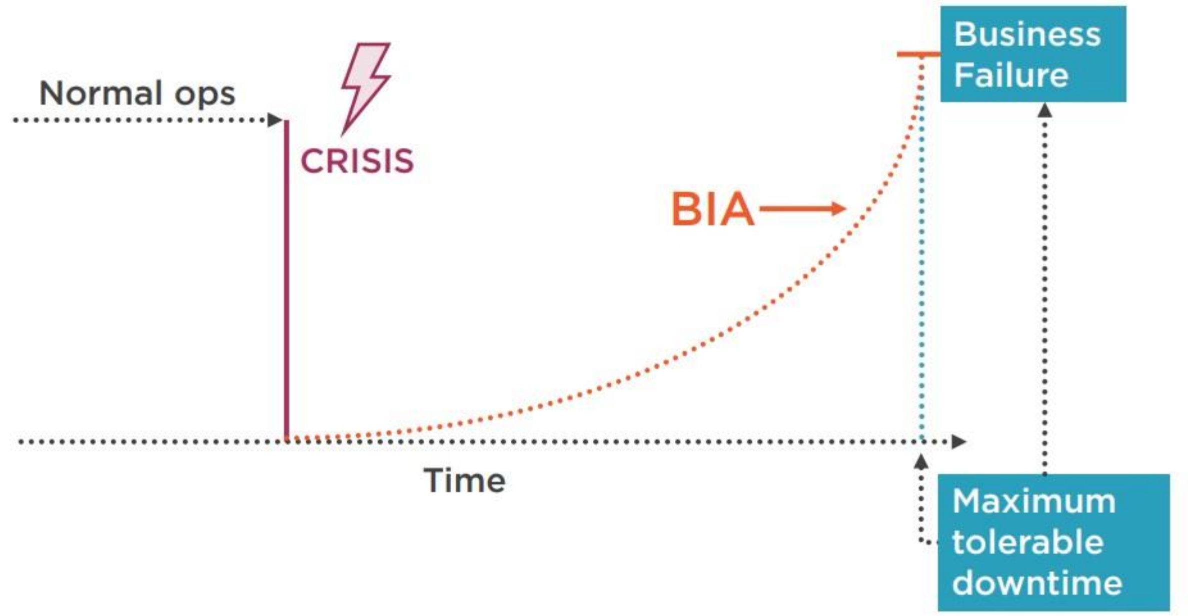
Introduction: Cybersecurity is a critical component of our overall information security strategy, aimed at protecting our organization's digital assets from cyber threats and attacks. This Cybersecurity Policy supplements the Information Technology Security Policy by providing specific guidelines and procedures for mitigating cyber risks and maintaining the resilience of our information systems.

Policy Statement: [Company Name] is committed to establishing and maintaining effective cybersecurity measures to safeguard its digital infrastructure, data assets, and operations against cyber threats. This policy applies to all employees, contractors, vendors, and any other parties with access to [Company Name]'s information systems and networks.

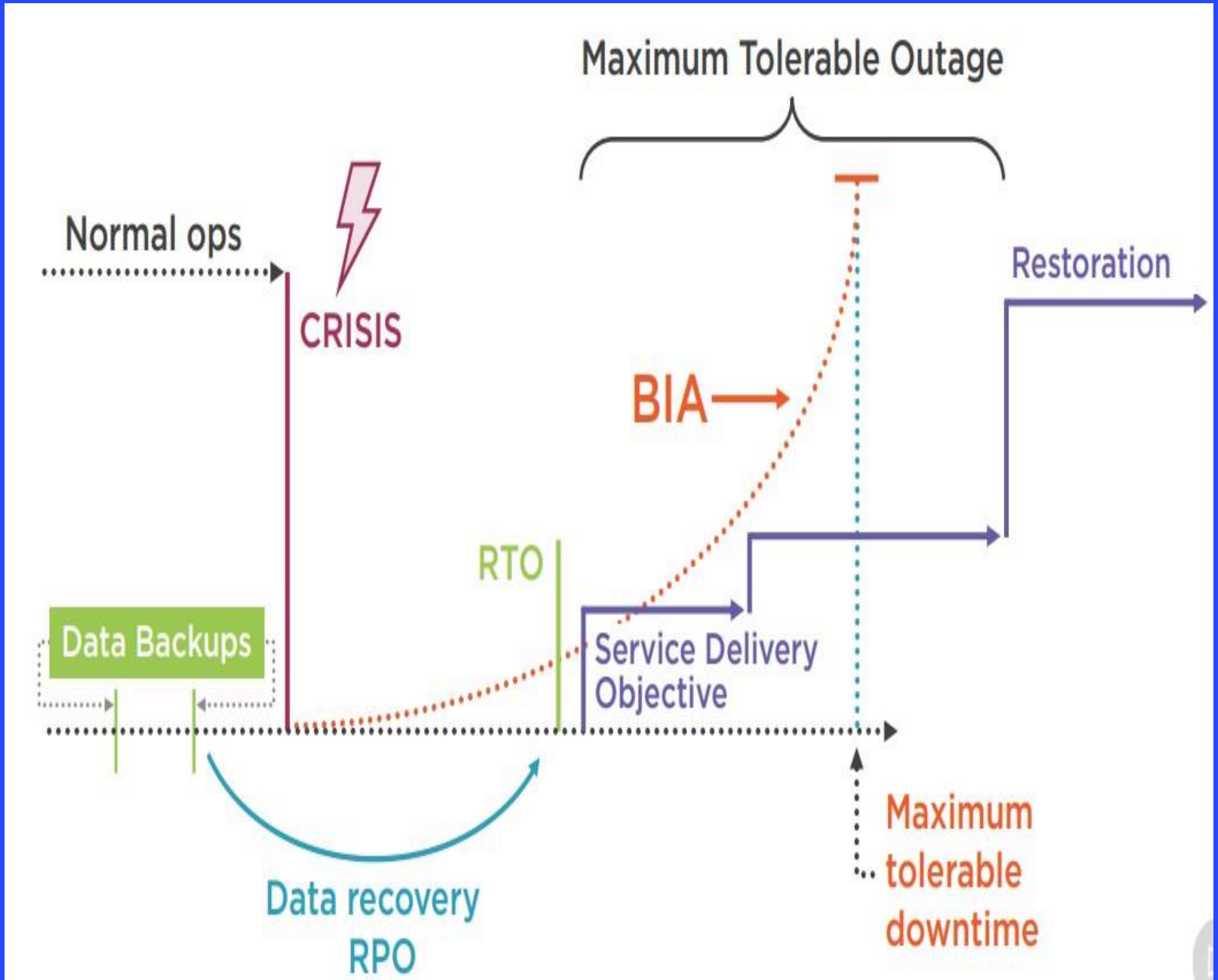
1. Risk Management: a. A formal risk assessment process shall be conducted regularly to identify, assess, and prioritize cybersecurity risks to the organization. b. Risk mitigation strategies shall be developed and implemented based on the assessment results, with appropriate controls and safeguards to address identified vulnerabilities and threats.
2. Cybersecurity Controls: a. Technical controls such as firewalls, intrusion detection/prevention systems, endpoint protection, and encryption shall be implemented to protect against unauthorized access, malware, and other cyber threats. b. Administrative controls such as access management, security awareness training, and incident response procedures shall be established to enforce security policies and procedures effectively.
3. Incident Response and Management: a. An incident response plan shall be developed, documenting procedures for detecting, reporting, and responding to cybersecurity incidents. b. A designated incident response team shall be trained and ready to respond promptly to cyber incidents, with predefined roles and responsibilities outlined in the incident response plan. c. Security incidents shall be investigated thoroughly, and appropriate actions taken to contain the incident, mitigate its impact, and restore normal operations as quickly as possible. d. Lessons learned from security incidents shall be documented and used to improve incident response procedures and strengthen cybersecurity defenses.
4. Data Protection and Privacy: a. Personal and sensitive data shall be protected in accordance with applicable laws, regulations, and industry standards, including data encryption, access controls, and data minimization principles. b. Privacy impact assessments shall be conducted for new projects, systems, or processes involving the collection, processing, or storage of personal data to identify and address privacy risks.
5. Third-Party Risk Management: a. Third-party vendors and service providers shall be assessed for their cybersecurity posture and adherence to security standards before engaging in business relationships. b. Contracts with third parties shall include provisions for cybersecurity requirements, data protection, and incident response obligations to mitigate risks associated with outsourcing or sharing data with external parties.
6. Security Awareness and Training: a. Employees shall receive regular cybersecurity awareness training to educate them about common cyber threats, phishing scams, social engineering tactics, and security best practices. b. Training materials and resources shall be made available to

Protect what’s most important.

- **Impact of Crisis Grows over Time (Business Impact Analysis - BIA)**
- **At some point the company is out of business**
- **Maximum Tolerable Downtime should be starting point for Information Security Policy.**
-



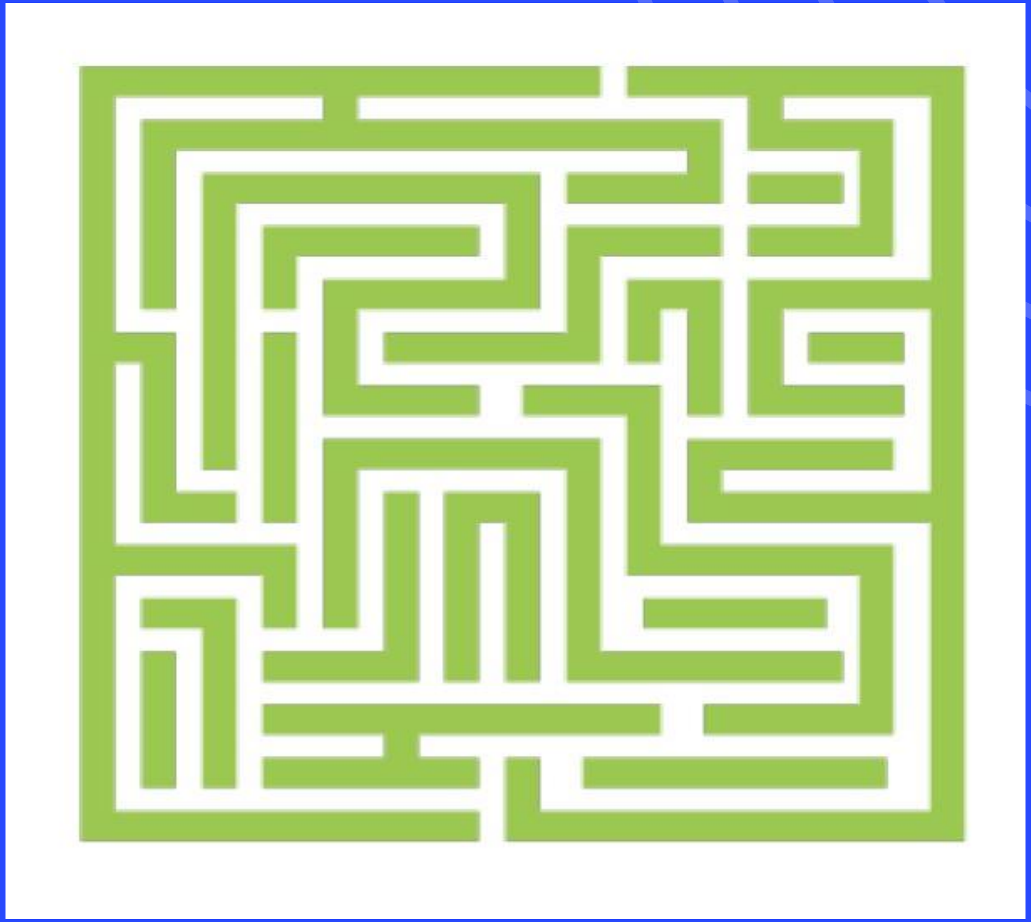
- Prioritize Mission Critical Services.
- Prioritize Degraded Services. (First to Restore).
- Part of Disaster Recovery Plan and Business Continuity Plan.
- Must also be Part of Cybersecurity Policy.
- Cyber Incident Response Team must be focused, staffed and funded accordingly.



Get an Assessment

Assessment Standards

- NIST
- CMMC
- CIS
- ITIL



Ancers can help.

No Sales Speak, Just information.

www.ancers.com