Importance of cybersecurity policies and procedures

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union
ncc.cy

Contents

TLP: WHITE

1 Introduction

- Cybersecurity policies and procedures are crucial for creating a secure organizational environment and protecting sensitive data.
- They ensure compliance with legal requirements and help mitigate risks from cyber threats.
- Organizations face threats like phishing, malware, ransomware, and insider threats.
- Strong cybersecurity policies help safeguard against these threats, ensuring business continuity.

2 Cybersecurity Policies

Acceptable Use Policy

TLP: WHITE

Defines acceptable use of organizational IT resources and systems.

Policy Elements:

- Users must use IT resources for authorized purposes only.
- Prohibited activities include accessing inappropriate content, illegal activities, and unauthorized sharing of sensitive information
- Consequences for policy violation

Password Policy

TLP: WHITE

Establishes requirements for creating and managing passwords

Policy Elements:

- Passwords must be at least 12 characters long and include a mix of letters, numbers, and special characters.
- Passwords must be changed every 90 days.
- Use of password managers is encouraged.
- Prohibition of sharing passwords.

Access Control Policy

Defines how access to information and systems is granted and managed

Policy Elements:

- Access based on the principle of least privilege.
- Role-based access control (RBAC) implementation.
- Regular review and revocation of access rights for former employees.

Data protection policy

Outlines measures for protecting sensitive data

Policy Elements:

- Data classification and handling guidelines
- Encryption requirements for data at rest and in transit
- Secure data disposal procedures

Incident Response Policy

TLP: WHITE

Provide guidelines for responding to cybersecurity incidents.

Policy Elements:

- Incident identification and reporting procedures.
- Roles and responsibilities of the incident response team.
- Steps for containing, eradicating, and recovering from incidents.

Remote Work Policy

TLP: WHITE

Sets requirements for secure remote work practises

Policy Elements:

- Use of VPNs for remote access
- Secure configuration of remote devices
- Guidelines for handling sensitive information outside the office

Vendor management policy

Ensures third-party vendors adhere to cybersecurity standards

Policy Elements:

- Vendor risk assessment and due diligence
- Security requirements in vendor contracts
- Regular monitoring and audits of vendor security practices

Email and communication policy

Defines secure use of email and communication tools.

Policy Elements:

- Use of secure communication channels
- Prohibition of sending sensitive information through unencrypted emails
- Phishing awareness and reporting procedures

3 Cybersecurity Procedures

Risk assessment and management

Systematic process for identifying, assessing, and mitigating risks

Procedure Steps:

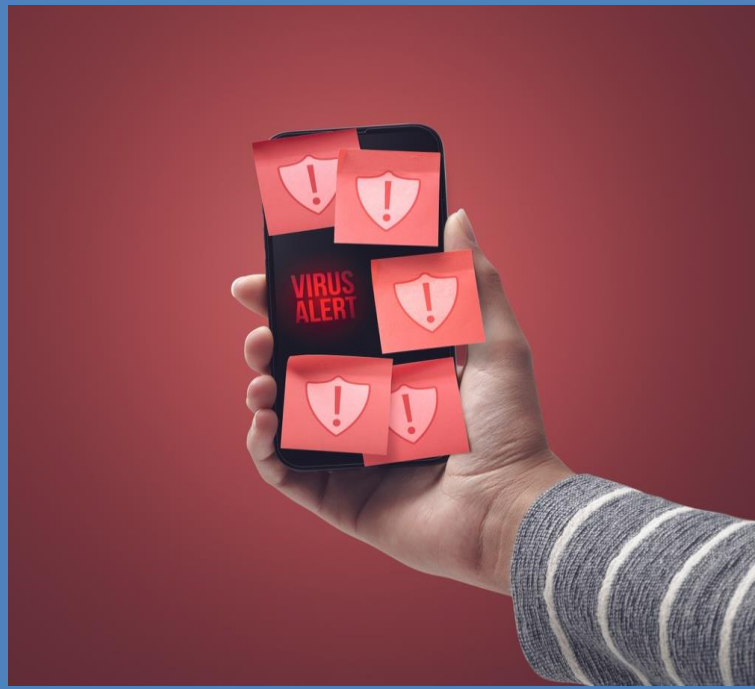
- Conduct regular risk assessments to identify potential threats
- Evaluate the likelihood and impact potential threats
- Develop and implement risk mitigation strategies
- Monitor and review risks periodically

Employee training and awareness

Implement training programs to educate employees on cybersecurity practices

Procedure steps:

- Conduct regular cybersecurity awareness training sessions.
- Implement phishing simulations and drills.
- Provide resources and materials on best practices and emerging threats.



Incident response procedures

Implement steps to take during a cybersecurity incidents

Procedure steps:

- Immediately report the incident to the incident response team.
- Isolate affected systems to prevent further damage.
- Conduct a preliminary assessment to understand the scope and impact
- Eradicate the threat and restore affected systems
- Document the incident and perform a post-incident review

Data backup and recovery procedures

TLP: WHITE

Ensuring data availability and integrity through regular backups

Procedure Steps:

- Implement automated backup solutions for critical data
- Store backups in secure, offsite locations
- Test backups and recovery processes regularly
- Document backup schedules and procedures

Software update and patch management

TLP: WHITE

Maintaining system security through regular updates

Procedure steps:

- Enable automatic updates for operating systems and applications
- Regularly review and apply security patches
- Maintain an inventory of software to track updates and vulnerabilities

Network security procedures

Protecting network infrastructure from unauthorised access

Procedure steps:

- Configure and maintain firewalls to control network traffic.
- Implement network segmentation to limit access to sensitive areas.
- Monitor network activity for suspicious behavior
- Conduct regular vulnerability assessments and penetration testing.

4 Risk management policies

Risk management policies

1. Risk Identification

Process of identifying potential cybersecurity risks

- Regularly review and update the risk inventory
- Engage stakeholders in risk identification activities
- Use threat intelligence to stay informed about emerging risks

2. Risk Assessment

Evaluating the likehood and impact of identified risks

- Conduct qualitative and quantitative risk assessments
- Prioritize risks based on their potential impact
- Document assessment findings and update risk registers

Risk management policies

3. Risk Mitigation

Implementing strategies to reduce risk exposure

- Develop and implement risk mitigation plans
- Assign risk ownership and accountability
- Monitor the effectiveness of mitigation strategies and adjust as needed

4. Risk Monitoring and Reporting

Ongoing monitoring and reporting of risk status

- Establish key risk indicators (KRIs) to monitor risk levels.
- Regularly review and update risk management reports
- Communicate risks status to senior management and stakeholders

5 Implementation and Compliance

Steps to implement cybersecurity policies and procedures

Guidance on rolling out cybersecurity measures

Implementation steps:

- Gain executive support and allocate resources
- Develop a detailed implementation plan with timelines and responsibilities
- Communicate policies and procedures to all employees
- Provide training and support to ensure understanding and compliance

Ensuring compliance and regular reviews

Maintaining adherence to policies and procedures

Compliance steps:

- Conduct regular audits and assessments to ensure compliance
- Use automated tools to monitor policy adherence
- Address non-compliance issues promptly and effectively

Continuous Improvement

Regularly updating and improving cybersecurity measures

Improvement steps:

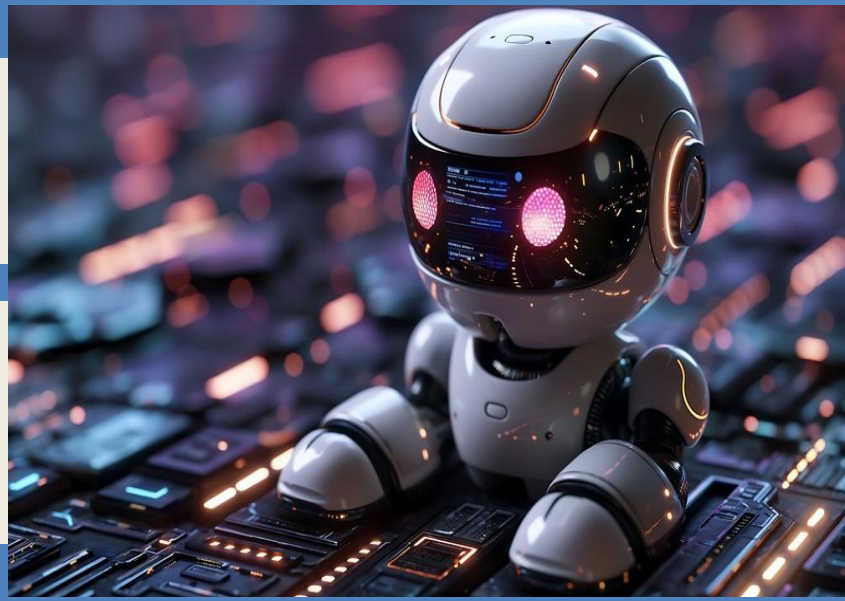
- Stay informed about new threats and best practices
- Solicit feedback from employees and stakeholders
- Regularly review and update policies and procedures

6 Resources and Tools

Recommended tools and solutions as well as government and industry resources

TLP: WHITE

List of tools to support cybersecurity efforts	• Antivirus Software • Firewalls • Encryption Tools • Backup Solutions
Links to useful resources and guidelines	• Cyprus Police Cybercrime Department • Cyprus Computer Emergency Response Team (CY-CERT) • European Union Agency for Cybersecurity (ENISA)



7 Conclusion

- Implementing strong cybersecurity policies is vital for safeguarding organizations from cyber threats and ensuring the protection of critical assets.
- Following the guidelines in this document enhances cybersecurity posture and maintains a secure environment through continuous improvement and regular reviews.
- The guide offers a comprehensive framework for establishing and maintaining effective cybersecurity policies and procedures.
- These guidelines help organizations mitigate risks, protect sensitive information, and improve overall cybersecurity.

Thank you!

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS

COMMISSIONER OF COMMUNICATIONS Digital Security Authority

Co-funded by the European Union

ncc.cy

References

- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14-30. https://doi.org/10.1016/j.cose.2015.11.001 (Introduction)
- Alhogail, A. (2020). Developing a cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003 (Cybersecurity Policies)
- Disterer, G. (2019). ISO/IEC 27000, 27001, and 27002 for information security management. *Journal of Information Security and Applications*, *46*, 27-37. https://doi.org/10.1016/j.jisa.2019.02.002 (Cybersecurity Procedures)
- Shedden, P., Ruighaver, A. B., & Ahmad, A. (2016). Risk management standards – The perception of ease of use. *Computers & Security*, *57*, 90-110. https://doi.org/10.1016/j.cose.2015.12.001 (Risk Management Policies)
- Tounsi, W., & Rais, H. (2020). A cybersecurity culture framework for assessing organization preparedness. *Journal of Information Security and Applications*, *53*, 102526. https://doi.org/10.1016/j.jisa.2020.102526 (Implementation and Compliance)
- Sari, A., & Azad, M. A. (2019). An integrated cybersecurity risk management approach for a cyber-physical system. *Journal of Information Security and Applications*, *46*, 193-208. https://doi.org/10.1016/j.jisa.2019.02.007 (Conclusion)