centralpoint
oxcyon

Cybersecurity Review Policy

Policy Statement:

This Cybersecurity Review Policy outlines the guidelines and procedures for conducting regular cybersecurity reviews within our organization. The objective of this policy is to ensure the ongoing assessment and improvement of our cybersecurity measures to protect sensitive information, systems, and assets from security threats and vulnerabilities.

1. Purpose and Scope:

1.1. Purpose: The purpose of this policy is to establish a systematic approach to regularly review and assess the effectiveness of our cybersecurity measures.

1.2. Scope: This policy applies to all employees, contractors, third-party vendors, and any other individuals who have access to our organization's information systems, data, and resources.

2. Policy Guidelines:

2.1. Frequency of Reviews:

- Regular cybersecurity reviews will be conducted annually as a minimum requirement.
- Additional reviews may be triggered by significant changes to our technology environment, regulatory requirements, or emerging threats.

2.2. Review Team:

- A dedicated cybersecurity review team will be established, consisting of qualified personnel from various departments, including IT, security, legal, and compliance.
- The team will be responsible for planning, executing, and documenting the cybersecurity reviews.

2.3. Review Objectives:

- The primary objectives of cybersecurity reviews are to Identify and assess security vulnerabilities and threats.
- Evaluate the effectiveness of existing security controls.
- Ensure compliance with relevant laws, regulations, and industry standards. Recommend improvements and remediation actions.

2.4. Risk Assessment:

- The review team will conduct a risk assessment to prioritize review areas based on potential impact and likelihood.

2.5. Review Areas:

- Cybersecurity reviews will encompass various areas, including but not limited to:
- Data protection
- Endpoint security
- Network security
- Access control
- Incident response
- Security awareness training
- Third-party vendor security
- Compliance with relevant regulations

2.6. Documentation:

- All cybersecurity reviews will be thoroughly documented, including findings, recommendations, and action plans.
- Documentation will be stored securely and made available to relevant stakeholders.

2.7. Action Plans:

- Action plans will be developed based on the review findings and recommendations.
- Responsible individuals and timelines for implementing corrective actions will be assigned.

3. Review Process:

3.1. Planning:

- The review team will create a review plan, including objectives, scope, methodology, and a schedule.

3.2. Execution:

- The review team will conduct the review activities, which may include interviews, assessments, testing, and documentation analysis.

3.3. Reporting:

- The review team will produce a comprehensive report summarizing findings, recommendations, and action plans.

- Reports will be shared with senior management and relevant stakeholders.

3.4. Remediation:

- Responsible individuals and departments will implement the recommended actions to address identified vulnerabilities and weaknesses.

3.5. Monitoring:

- Progress on remediation actions will be monitored and reported regularly until all actions are completed.

4. Review Continuity:

4.1. Lessons Learned:

- After each review, the cybersecurity review team will conduct a lessons learned session to improve the review process continually.

4.2. Adaptive Approach:

- The cybersecurity review process will adapt to changes in the threat landscape, technology environment, and regulatory requirements.

5. Compliance and Accountability:

5.1. Non-Compliance:

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

5.2. Accountability:

- Senior management is accountable for ensuring the effective implementation of this policy.

6. Policy Review:

This policy will be reviewed annually or as necessary to ensure its effectiveness and relevance. Changes to the policy will be made as needed to address emerging threats, industry best practices, and regulatory requirements.

7. Conclusion:

The cybersecurity review policy is a critical component of our overall cybersecurity program. Regular reviews will help us identify and mitigate security risks, enhance our security posture, and protect our organization's sensitive information and assets. All employees and stakeholders are expected to adhere to this policy to maintain the security and integrity of our organization's systems and data.

Policy Questions

All questions about this Policy or any other areas regarding Information Technology should be directed to the Chief Information Officer (CIO), who can be contacted at mkerchenski@oxcyon.com

Revision History

Date of Change	Responsible	Summary of Change
June 2023	Oxcyon Policy Team	No changes, semi annual review.