IFIN Global Group
Threat and Vulnerability Management Policy

1. Purpose

The purpose of this policy is to establish a framework for identifying, assessing, and managing threats and vulnerabilities within IFIN Global Group's IT environment. This policy aims to mitigate risks and protect the organization's assets from potential threats and vulnerabilities. It outlines the procedures and responsibilities for maintaining a robust security posture.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who have access to IFIN Global Group's IT resources. It covers all systems, applications, networks, and data, regardless of location. The policy ensures a unified and comprehensive approach to threat and vulnerability management across the organization.

3. Definitions

- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations, assets, or individuals through unauthorized access, destruction, disclosure, or modification of information. Examples include cyber-attacks, natural disasters, and insider threats.
- **Vulnerability:** A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Vulnerabilities can arise from software bugs, misconfigurations, or lack of proper security controls.
- **Threat and Vulnerability Management (TVM):** The process of identifying, evaluating, and mitigating threats and vulnerabilities to reduce risk. TVM involves continuous monitoring, assessment, and improvement to safeguard the organization's assets.

4. Objectives

- To identify and assess threats and vulnerabilities in a timely manner, ensuring that potential risks are addressed before they can impact the organization.
- To prioritize vulnerabilities based on risk and impact, allowing the organization to focus resources on the most critical areas.
- To implement measures to mitigate identified risks, thereby reducing the likelihood and impact of security incidents.
- To continuously monitor and improve the organization's security posture, adapting to new threats and vulnerabilities as they emerge.

5. Roles and Responsibilities

- **Chief Information Security Officer (CISO):** Oversees the TVM program and ensures alignment with organizational objectives. The CISO is responsible for the strategic direction and effectiveness of the TVM processes.

- **IT Security Team:** Conducts vulnerability assessments, manages threat intelligence, and implements mitigation strategies. The team ensures that identified threats and vulnerabilities are addressed promptly.
- **System Owners:** Ensure that their systems are compliant with TVM policies and address identified vulnerabilities. They are responsible for implementing and maintaining security controls on their respective systems.
- **Employees and Contractors:** Report any identified threats or vulnerabilities and follow the TVM procedures. All personnel play a crucial role in the early detection and reporting of potential security issues.

6. Threat and Vulnerability Management Process

6.1 Identification

- **Threat Intelligence:** Gather and analyze information from various sources about potential threats. This includes subscribing to threat intelligence feeds, monitoring security bulletins, and collaborating with industry peers.
- **Vulnerability Scanning:** Regularly scan systems and networks to identify vulnerabilities. Use automated tools to detect vulnerabilities and conduct manual reviews for thorough assessments.
- **Anti-Virus/Anti-Malware Detection:** Deploy and maintain anti-virus and anti-malware tools to detect and prevent malicious software. Ensure that these tools are updated regularly to recognize the latest threats.
- **Reporting:** Encourage reporting of potential threats or vulnerabilities by all employees and contractors. Provide clear guidelines on how to report incidents and ensure timely follow-up.

6.2 Assessment

- **Risk Assessment:** Evaluate the severity and potential impact of identified threats and vulnerabilities. Assessments should consider the likelihood of exploitation and the potential damage to the organization.
- **Prioritization:** Prioritize vulnerabilities based on their potential impact on the organization. Use a risk-based approach to allocate resources effectively, focusing on high-risk vulnerabilities first.

6.3 Mitigation

- **Remediation Planning:** Develop plans to address high-priority vulnerabilities. Plans should include specific actions, responsible parties, and timelines for remediation.
- **Implementation:** Apply patches, update configurations, and take other necessary actions to mitigate vulnerabilities. Ensure that mitigation efforts do not introduce new risks.
- **Risk Acceptance:** Document and formally accept residual risks that cannot be mitigated, after thorough evaluation and approval by senior management. Ensure that accepted risks are reviewed periodically.
- **Verification:** Test systems to ensure that vulnerabilities have been effectively addressed. Conduct follow-up assessments to confirm that mitigation measures are successful.

6.4 Monitoring and Review

- **Continuous Monitoring:** Implement continuous monitoring of systems for new threats and vulnerabilities. Use automated tools and regular audits to maintain an up-to-date security posture.
- **Regular Reviews:** Conduct periodic reviews and audits of the TVM process to ensure effectiveness. Reviews should assess the adequacy of existing controls and identify areas for improvement.
- **Incident Response:** Integrate TVM with the incident response process to handle threats that materialize. Ensure that incident response plans include procedures for addressing vulnerabilities.

6.5 Reporting Metrics

- **Identification Metrics:** Track the number of vulnerabilities identified, categorized by severity and type. Use these metrics to gauge the effectiveness of identification processes.
- **Remediation Metrics:** Measure the time taken to remediate vulnerabilities and the percentage of vulnerabilities mitigated within defined timeframes. These metrics help assess the efficiency of mitigation efforts.
- **Risk Metrics:** Monitor the number of accepted risks, including their severity and rationale for acceptance. Use these metrics to understand the organization's risk tolerance and decision-making processes.

7. Communication Plan

- **Internal Communication:** Keep relevant stakeholders informed about significant threats and vulnerabilities. Regular updates ensure that everyone is aware of potential risks and their mitigation status.
- **External Communication:** Communicate with customers, partners, and regulatory bodies as necessary regarding significant vulnerabilities and the steps taken to mitigate them. Transparency helps maintain trust and compliance.

8. Training and Awareness

- **Employee Training:** Provide regular training on threat and vulnerability management to all employees. Training should cover the identification, reporting, and mitigation of threats and vulnerabilities.
- **Awareness Programs:** Conduct awareness programs to keep employees informed about current threats and best practices for mitigating them. Regular updates help maintain a high level of vigilance and preparedness.

9. Continuous Improvement

- **Feedback Loop:** Incorporate feedback from vulnerability assessments and incident responses to improve the TVM process. Use lessons learned to refine procedures and enhance security measures.
- **Updates and Enhancements:** Regularly update TVM tools and methodologies to keep pace with evolving threats and vulnerabilities. Stay informed about industry best practices and technological advancements.

10. Compliance and Legal Requirements

- **Regulatory Compliance:** Ensure that the TVM process complies with relevant laws, regulations, and industry standards. Adherence to legal requirements helps avoid penalties and maintains organizational integrity.
- **Audits and Assessments:** Conduct regular audits to verify compliance with this policy and identify areas for improvement. Use audit findings to enhance the effectiveness of the TVM process.

11. Policy Review

- This policy will be reviewed annually or following any significant security incident to ensure its continued relevance and effectiveness. Regular reviews help adapt the policy to changing threats and organizational needs.