SHTP Cybersecurity Framework: User Guide

Version 1.0 Date: May 16, 2025

Table of Contents

1. Introduction to the SHTP Cybersecurity Framework

Welcome to the SHTP Cybersecurity Framework! This guide is designed to help you understand, navigate, and maximize the benefits of our comprehensive framework and its associated actionable tools.

Purpose and Goals: The SHTP Cybersecurity Framework aims to provide organizations with clear, actionable guidance to understand and mitigate cybersecurity risks associated with critical contemporary factors. Our primary goal is to empower you to enhance your cybersecurity posture by addressing specific challenges posed by areas such as: - The lasting impacts of COVID-19 on cybersecurity. - The emerging risks and opportunities of Generative AI (GenAI). - Compliance and operational requirements of the NIS2 Directive.

Overview of Key Areas Covered: The framework is structured around dedicated sections for each key factor, offering in-depth information and tailored advice.

2. Navigating the Framework Content

Our website is designed for easy access to all framework components.

Accessing Specific Factor Pages: You can typically find direct links to the COVID-19, GenAI, and NIS2 sections from the main navigation menu, often under headings like "Cybersecurity Factors" or similar.

Understanding Page Structure: Each factor page generally follows a consistent structure: - **Overview:** An introduction to the factor and its relevance to cybersecurity. - **Identified Risks:** A detailed breakdown of potential threats and vulnerabilities. - **Mitigation Strategies:** Recommended actions, best practices, and controls to address the identified risks. - **Actionable Tool(s):** Interactive assessments or navigators to help you apply the framework's principles directly to your organization. - **References & Resources:** Further reading and sources for the information provided.

3. Maximizing the Framework's Value

To get the most out of the SHTP Cybersecurity Framework:

Utilize Informational Sections: - **Understand the Risks:** Carefully review the "Identified Risks" sections for factors relevant to your organization. This will help you recognize potential vulnerabilities. - **Implement Mitigation Strategies:** The "Mitigation Strategies" provide practical steps. Prioritize these based on your risk assessment and organizational context.

Tailor Guidance: - The framework provides general best practices. Always adapt the recommendations to your specific industry, size, technological environment, and regulatory obligations. - Use the framework as a starting point for internal discussions and policy development.

---

4. Leveraging Actionable Tools

Our interactive tools are designed to provide personalized insights and guidance.

General Introduction: These tools typically involve answering a series of questions or inputting specific information about your organization. The output will help you understand your position concerning a particular risk or regulation.

4.1. NIS2 Applicability Navigator

```
- **Purpose:** Helps determine if your organization falls under the scope of the
NIS2 Directive.
- **How to Use:**
    1. Access the tool from the NIS2 factor page.
    2. Answer questions about your organization's sector, size, and services.
    3. The tool will provide an indication of whether NIS2 likely applies to you.
- **Interpreting Results:** The outcome is a preliminary assessment. If
applicability is indicated, consult legal and cybersecurity experts for formal
confirmation and next steps.
- **Benefits:** Quickly understand potential NIS2 obligations and focus compliance
efforts.
```

4.2. Interactive GenAI Risk Assessment

```
- **Purpose:** Assists in identifying and evaluating potential cybersecurity risks
associated with the use of Generative AI technologies.
- **How to Use:**
    1. Navigate to the tool from the GenAI factor page.
    2. Respond to prompts about your current or planned use of GenAI, data
handling practices, and existing security controls.
    3. The tool will highlight potential risk areas and may suggest relevant
mitigation strategies from the framework.
- **Interpreting Results:** Use the assessment to prioritize areas for deeper
investigation and to inform your GenAI adoption policies and security measures.
- **Benefits:** Proactively address GenAI-specific vulnerabilities and promote
responsible AI adoption.
```

4.3. Interactive AI Checklist (COVID-19 Context)

```
- **Purpose:** Provides a checklist to assess and enhance cybersecurity measures
related to AI technologies, particularly considering the operational shifts (e.g.,
remote work, accelerated digitalization) influenced by the COVID-19 pandemic.
- **How to Use:**
    1. Find the checklist on the COVID-19 factor page.
    2. Review each item, considering its relevance to your AI systems and post-
pandemic operational model.
    3. Identify gaps and areas for improvement in your AI security posture.
- **Interpreting Results:** The checklist helps ensure that AI systems deployed or
scaled during/after the pandemic are adequately secured against relevant threats.
- **Benefits:** Strengthen security for AI applications in the evolving work
environment, addressing risks highlighted by pandemic-driven changes.
```

5. Further Resources and Support

Website Resources Page: - Visit the dedicated "Resources" section on our website (often accessible from the main navigation). This page contains additional guides, articles, and links to support your cybersecurity efforts, including a guide on navigating the SHTP website itself.

Ongoing Improvement: - Cybersecurity is an evolving field. Regularly revisit the SHTP Cybersecurity Framework for updates and new information. - Foster a culture of security awareness within your organization.

6. Conclusion

The SHTP Cybersecurity Framework and its actionable tools are valuable resources for strengthening your organization's defenses against modern cyber threats. By actively engaging with the content and utilizing the interactive assessments, you can make informed decisions and implement effective cybersecurity measures.

We encourage you to use this guide as a companion in your journey towards a more secure digital environment.

End of Guide