Part 1: Development Process for BYOD Policy

Overview

We'll break this document into two. The first one will showcase the development of the BYOD Policy, and the second one will showcase the development of the Incident Response Policy. We used industry best practices and existing frameworks, along with policy development powered by AI, to create a security policy that is robust, complete, and can be implemented easily.

Development Methodology

Research and Framework Selection

To ensure our BYOD policy would align with industry best practices, we began by researching existing security frameworks and standards. We focused on:

- **NIST Special Publications**: especially NIST SP 1800-22 for the BYOD security guide.
- **SANS Policy Templates** to help write the policy.
- **The ISO 27001/27002 standard** to guide our overall structure & compliance considerations of the policy.
- **Sector-specific BYOD frameworks** to meet our own needs.

AI-Assisted Policy Development

Initial Policy Generation

With prompts outlining the unique requirements of our class project, we leveraged GPT-based AI tools to draft a BYOD policy. The policy's scope included:

- The policy's scope and its purpose.
- Important safety standards for mobile devices.
- Compliance requirements.
- Implementation and enforcement mechanisms.

Our BYOD policy prompt included requirements for:

- Device coding and login needs.

- Network security access and controls.
- Personal device usage policies.
- Privacy concerns for employee-owned devices.
- Security software requirements.
- Data segregation approaches.
- Incident reporting related to mobile devices.

Iterative Refinement

The first AI-generated draft was extensively revised through multiple iterations:

- We first asked the AI to review the policy for logical inconsistencies, contradictions, or unclear directives regarding BYOD management.
- We requested the AI to highlight possible security weaknesses in the BYOD plan and recommend changes for better device handling, data security, and access control.
- We refined the language and structure to make the policy clear, actionable, and easily understandable for all stakeholders.

Template Integration

Instead of creating a policy from scratch, we provided the AI with several existing BYOD policy templates:

- **SANS BYOD Security Policy Template**
- **NIST Guidance for Mobile Device Security for BYOD**
- **Information Security Forum (ISF) BYOD Templates**
- **Sample rules from mobile device management solution providers**

These templates helped us adopt best practices while customizing the policy to our class project's needs.

Group Review and Validation

After drafting the AI-based policy, our group conducted a thorough review:

- Each group member reviewed the BYOD policy.
- Team discussions addressed issues related to device management and data protection.
- We validated technical controls within our project scope.
- We ensured alignment with course requirements.

Policy Finalization

We compiled all feedback and finalized the BYOD policy with a focus on:

- Ensuring uniform style and terminology.
- Using clear section headings for better readability.

- Adding appendices for technical specifications.
- Establishing a system for policy updates.

Challenges and Solutions

Challenge: Balancing Security and Usability
Solution: We asked AI to propose security measures based on data type and user role, ensuring strong security without excessive restrictions.

Challenge: Addressing Privacy Concerns
Solution: We refined the policy to specify what can and cannot be monitored on personal devices and set clear procedures for data security.

Conclusion

We developed our BYOD policy by integrating human intelligence with AI. By combining best practices, frameworks, and AI-assisted drafting and refining, we created a comprehensive, user-friendly, and effective security policy tailored to our class project.

Part 2: Development Process for Incident Response Policy

Overview

This document outlines how our group developed a comprehensive Incident Response Policy for our Applied Network Security class project. Our approach integrated industry best practices, existing frameworks, and AI-assisted policy development to create an effective security framework.

Development Methodology

Research and Framework Selection

To ensure our policy adhered to best practices, we researched existing frameworks and standards, focusing on:

- **NIST Cybersecurity Framework**

- **SANS Incident Response Framework** (for process structuring)
- **CIS Controls**: Control 17 ensures a strong incident response framework.
- **ISO/IEC 27035**: Incident Management best practices.

AI-Assisted Policy Development

Initial Policy Generation

We utilized AI tools to draft an incident response policy covering:

- Scope and objective.
- Incident classification requirements.
- Response team structure and responsibilities.
- Compliance considerations.
- Implementation and enforcement mechanisms.

The policy prompt included requirements for:

- Incident classification and handling systems.
- Response team structure.
- Reporting and escalation procedures.
- Documentation and evidence collection requirements.
- Communication protocols during incidents.
- Post-incident investigations and learnings.
- Testing and training requirements.

Iterative Refinement

The AI-generated draft served as a foundation but required extensive refinement:

- AI was used to identify inconsistencies, contradictions, or unclear directives.
- AI-assisted gap identification in detection, containment, eradication, and recovery procedures.
- Language and structure were refined for clarity, enforceability, and usability by non-experts.

Template Integration

We leveraged existing incident response policy templates from reputable sources:

- **SANS Institute Incident Response Policy Template**
- **NIST Computer Security Incident Handling Guide (SP 800-61)**
- **CIS Control 17 Incident Response Policy Template**

These references helped adapt the policy from a broad standard to a specific class project framework.

Group Review and Validation

Our group conducted a detailed review:

- Each member reviewed the policy independently.
- Discussions addressed process and escalation concerns.
- We confirmed incident response strategies within our project scope.
- Ensured alignment with course requirements.

Policy Finalization

We compiled feedback and finalized the Incident Response Policy by focusing on:

- Maintaining consistent formatting and terminology.
- Structuring sections for logical flow.
- Adding appendices for incident response playbooks.
- Establishing review and update mechanisms.

Challenges and Solutions

Challenge: Creating Realistic Incident Response Procedures
Solution: AI-generated incident scenarios helped refine step-by-step procedures, ensuring they were neither too broad nor too rigid.

Challenge: Defining Appropriate Escalation Paths
Solution: AI-assisted decision trees outlined escalation protocols based on impact, scope, and sensitivity, which we refined to fit our project needs.

Conclusion

Our Incident Response Policy was developed through a combination of human expertise and AI-driven assistance. By leveraging industry best practices, formal frameworks, and iterative AI refinement, we created a comprehensive, practical, and effective security policy suitable for our Applied Network Security class project. Regular assessments and updates will ensure the policy remains relevant as cyber threats evolve.