**Plan of Action and Milestones (POA&M)**

1. **Document Information** 
   1. Document Title: CyberTech Innovations POA&M
   2. Version: 1.0
   3. Date:
   4. Prepared By: Tanasha Bryant
   5. Reviewer: Professor Frederick
2. **Executive Summary**

Purpose:

The purpose of this POA&M is to outline the corrective actions necessary to address identified security vulnerabilities and risks within CyberTech Innovations’ IT infrastructure. This plan will ensure compliance with NIST RMF guidelines and enhance the organization’s cybersecurity posture.

Scope:

The POA&M covers CyberTech Innovations’ key information systems, including:

* Customer Data Management System (CDMS)
* Research & Development (R&D) Network
* Supply Chain Management System (SCMS)
* Payment Processing System (PPS)

1. **Background**

Overview of Identified Issues:

A recent security assessment identified the following vulnerabilities:

* Phishing attacks targeting employee credentials (CDMS)
* Insider threats compromising proprietary research (R&D Network)
* Supply chain vulnerabilities leading to third-party data breaches (SCMS)
* Payment fraud risks in financial transactions (PPS)

Impact Analysis:

If left undressed, these vulnerabilities could result in data breaches, financial loss, regulatory penalties, and reputational damage.

1. **Objectives**

Goals:

* Mitigate security risks to ensure compliance with industry standards.
* Strengthen data protection and access controls.
* Improve incident response and threat detection mechanisms.

Expected Outcomes:

* Reduced likelihood of cyberattacks and data breaches.
* Enhanced operational resilience and business continuity.
* Improved compliance with cybersecurity frameworks.

1. **Action Plan** 
   1. Task Identification

|  |  |  |  |
| --- | --- | --- | --- |
| Task Number | Task Description | Responsible Party | Resources Required |
| 001 | Conduct phishing awareness training for employees. | IT Security Team | Training material instructor time. |
| 002 | Implement Zero Trust security model for R&D access. | IT Security & Compliance | Identity management tools, staff training |
| 003 | Perform third -party security audits for supply chain vendors | Vendor Management | Audit tools, external consultants |
| 004 | Deploy AI-based fraud detection for payment processing | Payment Security Team | AL fraud detection tools, budget allocation. |

* 1. Milestones

|  |  |  |  |
| --- | --- | --- | --- |
| Milestone Number | Milestone Description | Completion Date | Dependencies |
| M001 | Complete initial phishing training sessions. |  | None |
| M002 | Configure and test Zero Trust security controls |  | Task 002 |
| M003 | Finalize third-party security audits |  | Task 003 |
| M004 | Deploy AI fraud detection |  | Task 004 |

1. **Schedule**

A detailed timeline will outline the execution of tasks and milestones, ensuring timely implementation and risk mitigation.

Critical Path:

* Completion of phishing training is a prerequisite for access control improvements.
* Third-party security audits must be finalized before updating vendor contracts.
* AI fraud detection system implementation follows testing and approvals.

1. **Risk Management**

Risk Identification:

|  |  |  |
| --- | --- | --- |
| Risk | Description | Mitigation Strategy |
| Resistance to Training | Employees may not engage with security awareness training | Use gamification and incentives |
| Vendor Non-Compliance | Third-party vendors may not meet security standards. | Require compliance audits in contracts |
| Budget Constraints | Limited funding for new security tools | Prioritize critical security needs |

Risk Mitigation Strategies:

* Conduct periodic security awareness refreshers.
* Establish vendor security agreements.
* Allocate contingency funds for critical security measures.

1. **Monitoring and Reporting**

Progress Tracking:

* Utilize security dashboards and compliance tracking tools to monitor progress.
* Assign dedicated team members to oversee implementation.

Reporting Schedule:

* Monthly progress reports to executive leadership.
* Quarterly security assessments to validate mitigation effectiveness.

Review and Update Process:

* Biannual review of the POA&M to incorporate new threats and compliance updates.

1. **Approval**

Approval Signatures:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Title | Date | Signature | Initial |
|  | Chief Information Officer |  |  |  |
|  | IT Security Manager |  |  |  |
|  | Compliance Officer |  |  |  |
|  | Risk Management Lead |  |  |  |
|  | Audit Team Representative |  |  |  |

By signing this document, the individuals listed confirm that they have reviewed and approved the execution of this POA&M.