Multiple
United
Security
Assurance

BUSINESS PROPOSAL

Security Awareness Program Proposal

Prepared for Juliano Souza
Chief Information Security Officer
Date: 05/25/2025

Table of Contents

Executive Summary	3
Key Deficiencies Identified	4
Introduction	4
Purpose	4
Security Posture	5
Human Factors	6
Organizational Factors	6
Proposal	8
Human Factors: Unintentional Threats	8
Human Factors: Intentional Threats	10
Organizational Factors: Data Flow	11
Organizational Factors: Work Settings	14
Organizational Factors: Work Planning and Control	16
Organizational Factors: Employee Readiness	14
Budgetary Section	22
(PII) And Sensitive Data	25
Communication Plan	26
Messaging Strategies	26
Security Culture	27
Measuring Effectiveness	28
Long-Term Integration and Sustainability	29
Conclusion	30
References	31

Executive Summary

As the newly appointed Chief Information Security Officer (CISO) for Multiple United Security Assurance (MUSA) Corporation, I am presenting this security awareness program proposal to address the critical need for a robust and comprehensive approach to improving our organization's cybersecurity. The purpose of this proposal is to outline a strategic plan that will enhance our security posture, mitigate risks, and foster a healthy security culture across the organization. The information security team has highlighted the urgent need for such a program, and the current state of our security practices demands immediate action to protect our assets, data, and reputation. Multiple United Security Assurance (MUSA) Corporation faces significant cybersecurity risks due to a weak security posture characterized by inadequate policies, lack of employee training, and insufficient technical safeguards. This proposal outlines a comprehensive security awareness program to address these deficiencies, mitigate risks from both malicious and unintentional threats, and foster a robust security culture. The program includes targeted policies, a continuous monitoring framework, and a communication plan to engage stakeholders effectively. By addressing ten critical deficiencies—such as the absence of annual cybersecurity training, lack of intrusion detection systems, and poor configuration management, this initiative aims to reduce phishing success rates by up to 70% (KnowBe4, 2023) and align with industry standards like NIST SP 800-53 and 800-171. The proposed measures will enhance data protection, ensure regulatory compliance, and safeguard MUSA's reputation and operations.

Key Deficiencies Identified:

1. No annual cybersecurity awareness training, increasing vulnerability to phishing and social engineering.
2. Absence of an intrusion detection or prevention system, limiting threat detection capabilities.
3. No log collection or analysis, hindering incident response and monitoring.
4. Lack of encryption or hashing, exposing sensitive data to unauthorized access or tampering.
5. No media access control policy, allowing unchecked data movement via removable media.
6. Absence of configuration change management, increasing risks of disruptions.
7. No separation of duties or mandatory vacation policies, enabling potential insider threats.
8. Infrequent vulnerability assessments (every three years), leaving risks undetected.
9. High employee turnover and low morale, contributing to a disengaged workforce.
10. Lack of structured onboarding/offboarding processes, risking unauthorized access.

This proposal is divided into three sections: Introduction, Proposal, and Communication Plan, addressing human and organizational factors to build a resilient security framework.

I. Introduction

A. Purpose

The purpose of this security awareness program is to transform MUSA Corporation's cybersecurity approach by addressing critical deficiencies and fostering a proactive, vigilant workforce. The absence of annual cybersecurity training has led to successful phishing and social

engineering attacks, exploiting employee unawareness (KnowBe4, 2023). Similarly, the lack of intrusion detection systems and infrequent vulnerability assessments—conducted only every three years—leave MUSA blind to evolving threats (Verizon, 2023). These gaps expose the organization to preventable risks, such as data breaches and internal misconduct, which jeopardize operational integrity and client trust. By implementing this program, MUSA aims to reduce security incidents, enhance compliance, and establish a foundation for long-term resilience.

In the face of escalating cyber threats, organizations must adopt a continuous monitoring strategy that not only leverages technical solutions but also addresses human and organizational factors. This Continuous Monitoring Plan outlines a comprehensive framework to safeguard against malicious activities and unintentional threats. It focuses on strengthening workplace settings, improving employee readiness, and aligning security practices with cultural values, thus fostering a proactive and resilient cybersecurity posture (National Institute of Standards and Technology [NIST], 2011).

B. Security Posture

MUSA Corporation's security posture is weak, characterized by a reactive approach lacking foundational safeguards. A recent risk assessment reveals critical gaps: no intrusion detection or prevention system, no log collection or analysis, and no encryption or hashing policies, leaving data vulnerable to unauthorized access (Scarfone & Mell, 2007). The absence of a configuration change management policy increases the risk of disruptions, while a media access control policy gap allows unchecked data movement. Infrequent vulnerability assessments fail to provide a real-time risk picture, with organizations lacking regular assessments being 2.5 times more likely

to suffer breaches (Verizon, 2023). These deficiencies demand a comprehensive overhaul to align with industry standards and protect MUSA's assets.

C. Human Factors

Human factors significantly undermine MUSA's security climate. Unintentional threats stem from the lack of cybersecurity training, leaving employees ill-equipped to recognize phishing or social engineering tactics, as evidenced by successful attacks (SANS Institute, 2022). Low morale and high turnover, driven by inadequate readiness programs, further exacerbate vulnerabilities, as disengaged employees are less likely to follow protocols. Intentional threats are evident in high theft and security incident reports, amplified by the absence of separation of duties and mandatory vacation policies. Without these controls, malicious insiders have unchecked opportunities to exploit systems, necessitating robust training and accountability measures.

D. Organizational Factors

Several organizational factors contribute to MUSA Corporation's unhealthy security culture, impacting data flow, work setting, work planning and control, and employee readiness. Regarding *data flow*, the lack of encryption, hashing, and media access control policies allows sensitive information to move freely without protection, increasing the risk of breaches or tampering. In terms of *work setting*, the high turnover and low morale reflect a disengaged workforce, likely worsened by a lack of structured security training and support, creating an environment where security is deprioritized. For *work planning and control*, the absence of configuration change management and separation of duties policies indicates inadequate oversight, leaving systems vulnerable to both accidental misconfigurations and intentional sabotage. Finally, *employee*

readiness suffers due to the lack of training and preparedness programs, leaving staff ill-equipped to handle threats. Research by SANS Institute (2022) indicates that organizations lacking structured security training and oversight experience 40% more incidents tied to human error (SANS Institute, 2022). Together, these organizational deficiencies foster a culture of neglect and vulnerability, which this security awareness program aims to rectify through targeted policies and continuous improvement initiatives.

Organizational deficiencies contribute to an unhealthy security culture across four key areas:

- Data Flow: The lack of encryption, hashing, and media access control policies allows sensitive data to move unprotected, increasing breach risks (Ponemon Institute, 2023).
- Work Setting: High turnover and low morale, coupled with inadequate training, create an environment where security is deprioritized (SANS Institute, 2022).
- Work Planning and Control: No configuration change management or separation of duties policies leads to oversight gaps, risking misconfigurations or sabotage (NIST, 2020).
- Employee Readiness: The absence of structured training and preparedness programs leaves employees ill-equipped, with human error linked to 40% more incidents in untrained organizations (SANS Institute, 2022).

These factors necessitate targeted policies and continuous improvement to foster a secure organizational culture.

II. Proposal

A. Human Factors: Unintentional Threats

To address unintentional human errors, including cognitive, psychosocial, and cultural factors, the following policies and practices are proposed:

- *Cybersecurity Awareness Training Policy:* Mandates annual training for all employees, covering phishing, password security, data handling, incident reporting, and safe browsing. Training includes online modules, workshops, and simulated phishing exercises to enhance recognition of threats (SANS Institute, 2022). Compliance is enforced, with records maintained by the Security Department.

  Policy Statements:

  i. All personnel must complete mandatory cybersecurity awareness training annually.
  ii. Training content will include phishing and social engineering awareness, password security, data handling and protection, incident reporting procedures, and safe internet browsing.
  iii. Training will be delivered through online modules, workshops, and simulated phishing exercises to enhance practical application.
  iv. The Security Department will maintain records of training completion for all personnel.
  v. Failure to complete training may result in disciplinary action, including restricted system access until compliance is achieved.

  Rationale: Reduces phishing susceptibility by 70% through education (SANS Institute, 2022).

- *Structured Onboarding/Offboarding Processes Policy:* Implement immediate access provisioning and deprovisioning using tools like Azure AD to prevent unauthorized access by new or departing employees (Luther, 2023).

Policy Statements:

i. All new hires must complete initial cybersecurity training within the first week of onboarding, covering system access protocols and security responsibilities.
ii. Access provisioning will use automated tools like Azure AD to ensure secure, role-based access.
iii. Upon termination or role change, access will be immediately revoked through automated deprovisioning processes.
iv. Offboarding includes a mandatory exit checklist to ensure return of company devices and data.
v. Regular audits of access controls will be conducted quarterly to verify compliance.

Rationale: Prevents errors from unauthorized access (Luther, 2023).

- *Employee Engagement Survey Policy:* Conduct quarterly surveys to gauge employee awareness and address psychosocial factors like stress or disengagement, reducing errors due to inattention (Employer Culture Monitoring, 2024).

This policy directly addresses the lack of cybersecurity training, a key factor in unintentional threats like phishing and social engineering. By providing regular training, it improves employees' ability to recognize and avoid these threats (SANS Institute, 2022).

Policy Statements:

i. Quarterly engagement surveys will be conducted to assess employee awareness, stress levels, and security concerns.
ii. Surveys will be anonymous to encourage honest feedback and will include questions on training effectiveness and workplace stressors.
iii. Results will be analyzed by HR and the Security Department to identify areas for intervention.
iv. Action plans based on survey findings will be implemented within 30 days of each survey.
v. Survey participation is mandatory, with completion tracked to ensure broad input.

Rationale: Addresses psychosocial factors like stress, reducing inattention (SANS Institute, 2022).

B. Human Factors: Intentional Threats

To mitigate intentional threats, such as social engineering and insider misconduct, the following are proposed:

- *Separation of Duties and Mandatory Vacation Policy:* Critical functions are divided among multiple employees, and those in sensitive roles must take one continuous week of vacation annually, with activities reviewed to detect fraud (NIST, 2020). Job rotation during vacations ensures oversight.

  Policy Statements:

  i. Critical job functions will be divided among multiple employees to ensure no single individual controls all stages of a sensitive process.
  ii. Employees in sensitive positions (e.g., IT admins, financial staff) must take a minimum of one continuous week of vacation annually.
  iii. During vacations, responsibilities will be temporarily reassigned to another employee via job rotation.
  iv. Activities of employees on vacation will be reviewed by the Security Department to detect anomalies or fraudulent actions.
  v. Non-compliance with vacation or separation requirements will result in disciplinary review.

  Rationale: Limits insider fraud opportunities (NIST, 2020).

- *Incident Reporting Training Policy:* Integrate incident reporting into annual training, encouraging employees to report suspicious activities without fear, deterring insider threats (SANS Institute, 2022).

  Policy Statements:

  i. All employees must report suspicious activities or security incidents within 24 hours via a designated reporting portal or hotline.
  ii. Training on incident reporting will be integrated into annual cybersecurity awareness sessions, emphasizing a no-reprisal policy for reporters.
  iii. Reported incidents will be investigated by the Security Department within 48 hours, with findings documented and shared with relevant stakeholders.

iv. Anonymous reporting options will be available to encourage participation.
v. Failure to report known incidents may result in disciplinary action.

Rationale: Deters insider threats through vigilance (SANS Institute, 2022).

- *Behavioral Analytics Policy:* Deploy tools like Exabeam to monitor employee behavior for anomalies, such as unauthorized access attempts, enhancing detection of malicious intent (NIST, 2011).

Policy Statements:

i. User and Entity Behavior Analytics (UEBA) tools, such as Exabeam, will be deployed to monitor employee activities for suspicious patterns.
ii. Baseline behaviors will be established for each role, with anomalies (e.g., unusual access times) triggering alerts.
iii. Alerts will be reviewed by the Security Department within 24 hours, with escalation protocols for high-risk incidents.
iv. Data collected for analytics will comply with privacy policies and be securely stored.
v. Employees will be informed of monitoring practices during onboarding to ensure transparency.

Rationale: Detects malicious intent early (NIST, 2011).

These strategies reduce opportunities for insider threats and promote accountability.

C. Organizational Factors: Data Flow

To protect against inoperative data flow factors, the following policies address secure connections, data integrity, and communication:

- *Data Encryption and Hashing Policy:* Mandates encryption (e.g., TLS, HTTPS) for data in transit and at rest, with hashing to ensure integrity. Encryption authenticates sender-receiver connections, preventing eavesdropping, while hashing detects tampering (Ponemon Institute, 2023).

Policy Statements:

i. All data transmitted across networks must use secure protocols (e.g., TLS, HTTPS) to encrypt data in transit.
ii. Sensitive data stored on systems and devices must be encrypted using AES-256 or equivalent standards.
iii. Hashing algorithms (e.g., SHA-256) must be applied to verify data integrity, with automated checks for hash mismatches.
iv. Encryption keys will be securely managed through a centralized key management system, with access restricted to authorized personnel.
v. Regular audits of encryption and hashing compliance will be conducted quarterly.

Rationale: Prevents eavesdropping and tampering (Ponemon Institute, 2023).

- *Media Access Control Policy:* Requires authorization, malware scanning, and encryption for removable media, with secure disposal to prevent data leaks (Ponemon Institute, 2023).

Policy Statements:

i. Use of removable media (e.g., USB drives, CDs) requires prior authorization from management.
ii. All removable media must be scanned for malware using endpoint protection tools before connecting to company systems.
iii. Sensitive data on removable media must be encrypted using approved encryption standards.
iv. Personal removable media use on company systems is prohibited unless explicitly authorized.
v. Secure disposal of removable media will follow NIST guidelines to prevent data recovery.

Rationale: Stops unauthorized data leaks (Ponemon Institute, 2023).

- *Secure Communication Guidelines Policy*

Implement clear guidelines for secure data sharing, supported by training on proper data handling to address poor communication and ensure clarity (NIST, 2020).

Policy Statements:

i. Employees must verify recipient identities before sharing sensitive data, using secure channels like encrypted email or Microsoft Teams.
ii. Data-sharing protocols will be included in annual cybersecurity training, with practical exercises on secure communication.
iii. A centralized communication platform will be implemented to standardize data exchange and reduce miscommunication.
iv. Violations of communication protocols will trigger retraining and, if repeated, disciplinary action.
v. Quarterly reviews will assess communication effectiveness and update guidelines as needed.

Rationale: Reduces miscommunication errors (NIST, 2020).

These measures ensure secure, tamper-proof data flow and reduce miscommunication risks. Regular audits using tools like Wireshark will verify protocol compliance and detect connection anomalies. Training on secure data-sharing practices will further reinforce proper communication channels, reducing the risk of miscommunication due to unsecured connections.

To prevent data tampering or alteration, the policy requires hashing algorithms (e.g., SHA-256) to generate unique data fingerprints, enabling detection of any unauthorized changes during transit or storage (Ponemon Institute, 2023). Automated integrity checks will be integrated into data workflows, with alerts triggered for hash mismatches.

Monthly email campaigns and workshops will reinforce these guidelines with practical examples, such as avoiding unverified email attachments. Implementing a centralized communication platform, like Microsoft Teams with secure channels, will streamline data exchange and reduce errors caused by miscommunication, fostering a culture of clarity and accountability.

D. Organizational Factors: Work Settings

To address inoperative work settings, such as distractions or inadequate security practices, the following are proposed:

- *Zero Trust Architecture (ZTA) Policy:* Enforce identity and access verification using tools like Okta, minimizing unauthorized access risks (NIST, 2011).

  Policy Statements:

  i. All access to network resources requires identity and device verification using tools like Okta or Azure AD.
  ii. Multi-Factor Authentication (MFA) is mandatory for all system access, both on-site and remote.
  iii. Access requests will be logged and reviewed monthly to identify unauthorized attempts.
  iv. ZTA configurations will be audited quarterly to ensure compliance with NIST standards.
  v. Employees will receive training on ZTA principles during onboarding and annual refreshers.

  Rationale: Minimizes unauthorized access distractions (NIST, 2011).

- *Secure Remote Access Policy:* Implement VPNs (e.g., Palo Alto GlobalProtect) and MFA (e.g., Duo) to secure remote work environments (NIST, 2011).

  Policy Statements:

  i. Remote access requires VPN connections (e.g., Palo Alto GlobalProtect) with MFA enabled via tools like Duo.
  ii. Remote devices must meet security baselines, enforced by endpoint management tools like Microsoft Endpoint Manager.
  iii. Remote access logs will be monitored daily for anomalies, with alerts escalated to the Security Department.
  iv. Employees must complete remote work security training before receiving access.
  v. Non-compliant devices will be blocked from network access until remediated.

  Rationale: Secures remote environments (NIST, 2011).

- *Configuration Management Tools:* Use Microsoft Endpoint Manager to enforce secure system baselines, reducing misconfiguration risks (NIST, 2020).

  Policy Statements:

  i. Real-time threat monitoring will be implemented using tools like Microsoft Sentinel and Splunk to detect suspicious activities.
  ii. Monitoring systems will generate alerts for anomalies, with responses initiated within 24 hours.
  iii. Monitoring configurations will be updated monthly to incorporate new threat intelligence.
  iv. Employees will be trained on recognizing and reporting monitoring alerts during workshops.
  v. Logs from monitoring systems will be retained for one year to support incident investigations.

  Rationale: Prevents disruptions (NIST, 2020).

- *Security Monitoring Policy:* Deploy Microsoft Sentinel and Splunk for real-time threat detection, addressing insufficient monitoring practices (NIST, 2011).

  Policy Statements:

  i. Real-time threat monitoring will be implemented using tools like Microsoft Sentinel and Splunk to detect suspicious activities.
  ii. Monitoring systems will generate alerts for anomalies, with responses initiated within 24 hours.
  iii. Monitoring configurations will be updated monthly to incorporate new threat intelligence.
  iv. Employees will be trained on recognizing and reporting monitoring alerts during workshops.
  v. Logs from monitoring systems will be retained for one year to support incident investigations.

  Rationale: Enhances proactive security (Scarfone & Mell, 2007).

These strategies create a secure, distraction-free work environment, enhancing overall security. Quiet workspaces and designated focus hours will be established to reduce environmental distractions, supported by employee feedback surveys to identify specific issues. Regular

training on maintaining focus during security tasks will further enhance vigilance, ensuring employees prioritize secure behaviors in busy work settings.

A resource allocation review will identify gaps in hardware or software, ensuring employees have the tools needed for secure operations. Leadership training will improve management systems, promoting clear role definitions and accountability to streamline workflows and reduce errors caused by resource shortages or mismanagement.

Secure remote access via VPNs (e.g., Palo Alto GlobalProtect) and Multi-Factor Authentication (MFA) using Duo will protect work settings, particularly for remote employees (NIST, 2011). Bi-monthly workshops will train staff in recognizing and reporting security gaps, embedding robust practices into daily operations and creating a secure, proactive work environment.

E. Organizational Factors: Work Planning and Control

To protect against inoperative work planning factors, such as job pressure or poor task management, the following are proposed:

- *Configuration Change Management Policy:* Requires formal change requests, approval, testing, and documentation to prevent disruptions and ensure oversight (NIST, 2020).

  Policy Statements:

  i. All changes to hardware, software, or networks must be submitted via a formal change request process, detailing impact and reason.
  ii. Changes require approval from designated personnel based on risk assessment.
  iii. Implementation must follow a documented plan with testing and back-out procedures.

iv. All changes will be documented, including who, when, and why, with records retained for one year.
v. Emergency changes follow an expedited process with mandatory post-implementation documentation.

Rationale: Prevents disruptions (NIST, 2020).

- *Task Management Platforms Policy:* Use Jira or Trello to streamline task allocation, reducing pressure and improving planning (Luther, 2023).

Policy Statements:

i. Task allocation will use platforms like Jira or Trello to prioritize and track workloads, ensuring clarity and balance.
ii. Managers must review task assignments weekly to prevent overload and align with employee capabilities.
iii. Employees will receive training on task management tools during onboarding.
iv. Task completion metrics will be reviewed monthly to identify planning gaps.
v. Non-compliance with task management protocols may result in retraining or reassignment.

Rationale: Reduces job pressure (Luther, 2023).

- *Job Rotation and Cross-Training Policy:* Implement rotation to minimize monotony and uncover skill gaps, enhancing control and resilience (Luther, 2023).

Policy Statements:

i. Employees in critical roles will participate in job rotation every six months to enhance skills and flexibility.
ii. Cross-training programs will be conducted quarterly to address skill gaps and prepare for routine changes.
iii. Training progress will be tracked, with completion required for role continuation.
iv. Managers will document rotation schedules and ensure coverage during transitions.
v. Feedback from rotations will be collected to improve training effectiveness.

Rationale: Enhances resilience (Luther, 2023).

- *Wellness Programs Policy:* Offer stress management and recognition programs to boost morale and reduce errors due to fatigue or dissatisfaction (Employer Culture Monitoring, 2024).

Policy Statements:

i. Wellness programs, including mindfulness sessions and health screenings, will be offered quarterly to address stress, fatigue, and illness.
ii. Employees must report health-related impairments affecting security tasks to HR confidentially.
iii. Flexible break schedules and ergonomic workspaces will be provided to reduce fatigue and boredom.
iv. Program participation will be encouraged through incentives like wellness credits.
v. Annual health and wellness surveys will assess program effectiveness and employee needs.

Rationale: Enhances readiness (Luther, 2023).

These measures improve oversight and support a balanced, secure work environment. Flexible scheduling and wellness programs, including stress management workshops, will mitigate pressure-related lapses, fostering a balanced work environment. Regular performance reviews will ensure tasks align with employee capabilities, minimizing overwhelm and enhancing adherence to security protocols.

Cross-training programs will prepare employees for routine changes, reducing errors due to unfamiliar tasks. Quarterly planning sessions will align tasks with organizational goals, using tools like Trello to improve task clarity and oversight, ensuring effective management and control.

The Cybersecurity Awareness Training Policy will include role-specific modules to address skill gaps, supported by upskilling programs via platforms like KnowBe4 (Employer Culture

Monitoring, 2024). Ongoing mentorship and feedback loops will ensure continuous skill development, empowering employees to handle security tasks confidently and competently.

F. Organizational Factors: Employee Readiness

To address inoperative employee readiness factors, such as inattention or lack of skills, the following are proposed:

- *Quarterly Cybersecurity Training policy:* Deliver sessions via KnowBe4, including phishing simulations and real-world scenarios to maintain engagement (Employer Culture Monitoring, 2024).

  Policy Statements:

  i. Employees must complete quarterly training sessions via platforms like KnowBe4, including phishing simulations and scenario-based exercises.
  ii. Training content will cover PII protection, incident reporting, and role-specific security tasks.
  iii. Completion will be tracked, with non-compliance resulting in restricted system access.
  iv. Training effectiveness will be evaluated through post-training quizzes and simulation outcomes.
  v. Feedback from employees will be collected to refine training content quarterly.

  Rationale: Maintains engagement (SANS Institute, 2022).

- *Career Growth Opportunities Policy:* Provide upskilling programs to enhance skills and reduce disengagement, lowering risks of errors or malicious acts (Luther, 2023).

  Policy Statements:

  i. MUSA Corporation will implement upskilling programs, including online courses and workshops via platforms like KnowBe4 and LinkedIn Learning, to enhance employee skills in cybersecurity and role-specific competencies.

ii. All employees will have access to at least one upskilling opportunity per quarter, tailored to their job functions and career goals.
iii. Career growth plans will be developed during annual performance reviews, with managers identifying skill gaps and recommending relevant training.
iv. Completion of upskilling programs will be tracked, with participation linked to performance evaluations and promotion eligibility.
v. Feedback on program effectiveness will be collected semi-annually to ensure alignment with employee needs and organizational security objectives.

Rationale: Reduces disengagement (Luther, 2023).

- *Wellness and Feedback Mechanisms Policy:* Implement stress reduction programs and ongoing surveys to address fatigue, boredom, and inattention, fostering readiness (Luther, 2023).

Policy Statements:

i. Quarterly wellness programs, including mindfulness workshops, stress management sessions, and access to mental health resources, will be provided to address employee stress, fatigue, and inattention.
ii. Ongoing employee feedback surveys will be conducted bi-monthly to assess workplace stressors, boredom, and security awareness, with anonymous responses encouraged to ensure candor.
iii. Survey results will be analyzed by HR and the Security Department within 15 days, with action plans developed to address identified issues.
iv. Flexible break schedules and ergonomic workspace adjustments will be implemented to reduce physical and mental fatigue, with compliance monitored by facility managers.
v. Participation in wellness programs will be incentivized through wellness credits or recognition, with annual evaluations of program impact on employee readiness.

- *Incident Reporting Culture policy:* Encourage reporting through training and an open environment, reducing risks from undetected issues (NIST, 2020).

Policy Statements:

i. All employees must report suspicious activities or security incidents within 24 hours via a designated online portal or confidential hotline, with training on reporting procedures included in quarterly cybersecurity sessions.
ii. A no-reprisal policy will be enforced to protect employees who report incidents in good faith, communicated during onboarding and annual training.
iii. Reported incidents will be investigated by the Security Department within 48 hours, with findings documented and shared with relevant stakeholders as needed.
iv. Anonymous reporting options will be available to encourage participation, with access restricted to authorized security personnel.
v. The Security Department will publish quarterly reports summarizing incident trends and resolutions to reinforce the importance of reporting and maintain transparency.

Rationale: Reduces undetected risks (NIST, 2020).

These strategies build a skilled, attentive workforce committed to security. Wellness programs, including mindfulness sessions and stress reduction workshops, will address psychological barriers, reducing inattention caused by stress (Luther, 2023). Regular engagement surveys will identify stressors, enabling targeted interventions to keep employees alert and security conscious.

Job rotation will reduce monotony, keeping employees engaged and vigilant (Luther, 2023). Health screenings and clear policies on reporting illness-related impairments will ensure employees are fit for security-critical tasks, reducing risks from diminished readiness.

Leadership modeling and “security champions” will promote positive attitudes toward security, aligning employee values with organizational goals (Employer Culture Monitoring, 2024). Transparent communication via monthly newsletters will reinforce the importance of security, encouraging a shared commitment to protecting MUSA’s assets and fostering a proactive mindset.

Budgetary Section

The estimated costs for the proposed security awareness program are as follows:

1. Cybersecurity Awareness Training:
   - Annual training modules: $10,000
   - Workshops and simulated phishing exercises: $5,000
   - Total: $15,000

2. Structured Onboarding/Offboarding Processes:
   - Azure AD tools: $3,000
   - Access provisioning and deprovisioning: $2,000
   - Total: $5,000

3. Employee Engagement Surveys:
   - Quarterly surveys: $1,000
   - Analysis and action plans: $2,000
   - Total: $3,000

4. Separation of Duties and Mandatory Vacation:
   - Implementation and monitoring: $2,000
   - Total: $2,000

5. Incident Reporting Training:
   - Annual training integration: $1,000
   - Total: $1,000

6. Behavioral Analytics:
   - Exabeam tools: $5,000
   - Monitoring and analysis: $3,000
   - Total: $8,000

7. Data Encryption and Hashing:
   - Encryption protocols: $4,000
   - Hashing algorithms: $2,000
   - Total: $6,000

8. Media Access Control:

- Authorization and malware scanning: $2,000
- Secure disposal: $1,000
- Total: $3,000

9. Secure Communication Guidelines:

- Training and implementation: $2,000
- Total: $2,000

10. Zero Trust Architecture:

- Okta tools: $5,000
- Multi-Factor Authentication: $3,000
- Total: $8,000

11. Secure Remote Access:

- VPNs and MFA: $4,000
- Endpoint management: $3,000
- Total: $7,000

12. Configuration Management Tools:

- Microsoft Endpoint Manager: $3,000
- Total: $3,000

13. Security Monitoring:

- Microsoft Sentinel and Splunk: $5,000
- Total: $5,000

14. Task Management Platforms:

- Jira or Trello: $2,000
- Total: $2,000

15. Job Rotation and Cross-Training:

- Implementation and monitoring: $2,000
- Total: $2,000

16. Wellness Programs:

- Stress management and health screenings: $3,000
- Total: $3,000

17. Quarterly Cybersecurity Training:

- KnowBe4 platform: $4,000
- Total: $4,000

18. Career Growth Opportunities:

- Upskilling programs: $3,000

- Total: $3,000

Overall Total Estimated Cost: $90,000

19. Wellness and Feedback Mechanisms:

- Mindfulness workshops and surveys: $2,000

- Total: $2,000

20. Incident Reporting Culture:

- Training and implementation: $2,000

- Total: $2,000

Protection of Personally Identifiable Information (PII) and Sensitive Data

The protection of Personally Identifiable Information (PII) and sensitive data is crucial for maintaining the integrity and trust of MUSA Corporation. The following measures are proposed to safeguard such information:

1. Data Encryption:
   - All PII and sensitive data must be encrypted using AES-256 or equivalent standards to prevent unauthorized access during transmission and storage.

2. Access Controls:
   - Implement role-based access controls to ensure that only authorized personnel can access PII and sensitive data.
   - Use Multi-Factor Authentication (MFA) to add an extra layer of security for accessing sensitive information.

3. Regular Audits:
   - Conduct regular audits of access logs and encryption protocols to ensure compliance and detect any unauthorized access attempts.

4. Employee Training:
   - Include PII protection in the annual cybersecurity awareness training, emphasizing the importance of handling sensitive information securely.
   - Provide practical exercises on recognizing and reporting potential breaches involving PII.

5. Secure Communication:
   - Use secure communication channels, such as encrypted email and Microsoft Teams, for sharing PII and sensitive data.
   - Verify recipient identities before transmitting sensitive information.

6. Incident Reporting:
   - Encourage employees to report any suspicious activities or potential breaches involving PII through a designated reporting portal or hotline.
   - Investigate reported incidents promptly and take corrective actions to mitigate risks.

By implementing these measures, MUSA Corporation can ensure the protection of PII and sensitive data, thereby maintaining compliance with regulatory standards and safeguarding the organization's reputation.

III. Communication Plan

A. Messaging Strategies

To ensure stakeholder comprehension and buy-in, tailored messaging strategies are proposed:

- *Senior Leadership:*
  - Risk Reports: Quarterly executive summaries highlight internal and industry incidents, linking to financial and reputational impacts (e.g., $2 million fines from PII breaches) (IBM Security, 2024).
  - Cost-Benefit Analysis: Data-driven dashboards show training reduces incidents by up to 70%, avoiding fines and enhancing compliance (KnowBe4, 2023; NIST, 2020).
  - Benchmarking: Case studies from peers demonstrate improved metrics post-training (NIST, 2018).
  - Delivery: Presented during strategic meetings with infographics for clarity.
- *Nontechnical Employees:*
  - Interactive Training: Bi-monthly workshops simulate phishing scenarios involving PII, making risks relatable (NIST, 2012).
  - Multimedia Content: Short videos and infographics on PII handling and best practices, delivered monthly via email (NIST, 2012).
  - Real-Life Examples: Anonymized breach stories (e.g., phishing leading to customer data exposure) highlight consequences (IBM Security, 2024).

- Personal Relevance: Emphasize protecting personal PII to prevent identity theft, fostering engagement (NIST, 2012).

Communication Channels and Frequency:

Audience	Channel	Frequency	Content Type
Senior Leadership	Executive Reports, Briefings	Quarterly	Dashboards, Cost Reports
All Employees	Email Campaigns	Monthly	Tips, Policy Updates
Nontechnical Staff	Workshops, Infographics	Bi-monthly	Scenario Exercises, Posters
New Hires	Orientation Training	At Onboarding	Compliance Policies, Basic Do's/Don'ts

B. Security Culture

A healthy security culture is critical for MUSA's resilience, as awareness alone is insufficient without behavioral change (NIST, 2020). The need is justified as follows:

- Shared Responsibility: Positioning security as everyone's role, from front desk to executives, fosters accountability. For example, encouraging PII reporting prevents breaches (NIST, 2012).
- Reward Programs: Recognize employees for reporting phishing or completing training early with digital badges or gift cards, boosting morale (Luther, 2023).

- Peer Influence: Appoint "security champions" to advocate best practices, enhancing peer-driven compliance (Employer Culture Monitoring, 2024).
- Gamification: Quizzes and leaderboards make learning engaging, reinforcing PII protection and vigilance (NIST, 2020).
- Measurable Impact: A strong culture reduces incidents by 40% and improves response times, protecting MUSA's reputation and finances (SANS Institute, 2022).

Measuring Effectiveness

Measurement is critical to ensure that communication efforts are yielding tangible results. The plan will incorporate both **quantitative** and **qualitative** metrics:

Key Performance Indicators (KPIs):

- Training Completion Rates: Percentage of employees who finish mandatory training modules on time, including modules on PII and sensitive information.
- Phishing Simulation Outcomes: Click-through rates and report rates during simulated phishing tests, particularly those involving PII-related scenarios.
- Help Desk Metrics: Reduction in user-caused security incidents (e.g., PII exposures) and increase in proactive security-related inquiries.
- Survey Feedback: Employee perception of cybersecurity relevance, understanding of PII/sensitive information, and confidence in protecting such data post-training.

Periodic reporting of these metrics will be delivered to executive leadership to demonstrate progress and identify areas for improvement.

Long-Term Integration and Sustainability

Sustainability requires moving from program-based thinking to lifecycle-based integration. The communication plan must ensure that security awareness, including protection of PII and sensitive information, is not treated as an annual campaign but as a core component of employee development and operational governance.

- Annual Reviews: Updating content and delivery methods based on changing threat landscapes, new types of PII/sensitive information risks, and employee feedback.
- Policy Alignment: Ensuring awareness messaging aligns with updated policies and NIST frameworks such as SP 800-53 and SP 800-171, which advocate for continuous personnel training and security education (NIST, 2020; NIST, 2018).
- Cross-Functional Integration: Collaborating with departments such as HR, Compliance, and Legal to embed security into onboarding, exit processes, and policy enforcement.

This approach persuades nontechnical audiences by linking security to personal and organizational benefits, ensuring cultural adoption.

Conclusion

This security awareness program proposal addresses MUSA Corporation's critical deficiencies through targeted policies, continuous monitoring, and a robust communication plan. By mitigating human and organizational risks, implementing technical safeguards, and fostering a proactive security culture, MUSA can reduce vulnerabilities, ensure compliance, and protect its assets. Continuous evaluation and stakeholder engagement will sustain long-term resilience. By tailoring messaging strategies for senior leadership (emphasizing breach costs and ROI) and nontechnical staff (clarifying PII and sensitive information), and by emphasizing personal relevance and organizational risk, the plan fosters an inclusive and proactive security culture. As the cyber threat landscape continues to evolve, continuous communication, measurement, and leadership engagement will be crucial in maintaining a resilient, security-conscious workforce.

References:

1. Employer Culture Monitoring. (2024). *Employee engagement and cybersecurity: Building a secure workforce*. Retrieved from https://www.rightpoint.com/landing-pages/agentic-workplace-employees-and-ai-power-the-future-of-work
2. IBM Security. (2024). *Cost of a data breach report 2024*. https://www.ibm.com/reports/data-breach
3. KnowBe4. (2023). *2023 phishing by industry benchmarking report*. https://www.knowbe4.com/phishing-benchmarking-report
4. Luther, D. (2023, November 30). *15 tips to reduce employee turnover and improve hiring and retention in 2024*. https://www.netsuite.com/portal/resource/articles/human-resources
5. National Institute of Standards and Technology. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations (NIST SP 800-137)*. https://doi.org/10.6028/NIST.SP.800-137
6. National Institute of Standards and Technology. (2012). *Computer security incident handling guide (NIST SP 800-61, Rev. 2)*. https://doi.org/10.6028/NIST.SP.800-61r2
7. National Institute of Standards and Technology. (2018). *Protecting controlled unclassified information in nonfederal systems and organizations (NIST SP 800-171, Rev. 2)*. https://doi.org/10.6028/NIST.SP.800-171r2
8. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (NIST SP 800-53, Rev. 5)*. https://doi.org/10.6028/NIST.SP.800-53r5
9. Ponemon Institute. (2023). *2023 cost of a data breach report*. IBM Security. https://www.ibm.com/reports/data-breach

10. SANS Institute. (2022). *2022 security awareness report: Managing human cyber risk*. https://www.sans.org/security-awareness-training/reports/2022-security-awareness-report

11. Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS) (NIST SP 800-94)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

12. Verizon. (2023). *2023 data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/