SECURITY PLAN

A logo with a shield and a sword

Description automatically generated

SALARY AND PERFORMANCE MANAGEMENT SYSTEM

The Triple Threat

(Team 2)

This Security Plan is designed for IT Management, the security team, and both the infrastructure and development teams involved in the Salary and Performance Management System.

**Overview:**

1. In developing the new Salary and Performance Management System, one of our primary concerns is ensuring the utmost security for sensitive information. The system is designed with layers of encryption to safeguard details such as employee salaries and performance reviews, ensuring that only authorized individuals have access.
2. Access is granted through a combination of secure password protocols and multi-factor authentication for an added layer of protection. We monitor everything happening in our system, logging every user interaction for transparency. Our security extends to user access, with strong policies like having a unique ID with 6 digits, distributed across the company with no similarity between two IDs.
3. Making sure our system is always up and running is also a top priority. We've got backup plans in place to minimize any downtime, and if something does go wrong, we have a quick and efficient recovery plan. Ensuring data accuracy is crucial, so we have validation tools and regular backups to prevent any losses.
4. Regular updates keep the system in check and fix any known issues. Following data protection rules is key for keeping things safe. Making sure the team knows how to stay safe is a big deal. Training programs teach the best ways to work securely and spot potential issues, keeping us ahead of any cybersecurity challenges.
5. Our approach to the new Salary and Performance Management System is grounded in a comprehensive security framework, ensuring confidentiality, integrity, and availability of critical information while adhering to industry standards and regulatory requirements. Continuous reviews and updates are important to adapting our security measures to evolving technological landscapes and emerging threats.

**Introduction/Management Summary:**

* The primary goal is to make sure to keep all the important details of the Salary and Performance Management System safe and secure.
* The system efficiently manages salary and performance data. Security is a top priority to keep this sensitive information safe and secure. The focus is on maintaining confidentiality and accuracy throughout the system's operations.
* We're setting clear boundaries for our system. In the scope are crucial aspects like employee performance reviews (both projections and actuals), employee salary details (projections and actuals), Quality Performance Reviews (QPR), data storage and retrieval, user authentication and authorization, reporting, notifications, and necessary employee data related to salary and performance management. Anything beyond these key elements falls out of scope, helping us stay focused on what's essential for effective salary and performance management. Out of scope are areas such as HR & Payroll, tax-related functions, legal compliance (handled externally by the legal department), and any employee personal data beyond what's necessary for salary and performance management. This ensures that our system stays focused on its primary functions without delving into areas outside its intended scope.
* Few assumptions for our system:

We expect a reliable and scalable infrastructure.

Users are assumed to follow standard security protocols.

External services, like data storage, are expected to be consistently available. These assumptions guide our planning and approach to development.

This Security Plan for the Salary and Performance Management System is strategically designed to ensure the Confidentiality, Integrity, and Availability (CIA) of sensitive data.

**Confidentiality:**

* Sensitive data, such as salary details and performance reviews, is encrypted to ensure only authorized individuals have access.
* The server hosting the system is securely placed in a cloud-based environment, enhancing data security.
* Strict access controls, including robust authentication methods, are implemented to prevent unauthorized entry.
* Access controls are fine-tuned, allowing employees and managers varied levels of access based on their roles and responsibilities.
* Specific user permissions are granted depending on departmental affiliations or supervisory roles, ensuring confidentiality in line with jurisdiction.

**Integrity:**

* Management holds read and write privileges for file access, with restrictions placed post-approval of projections to prevent unauthorized changes.
* Staff hold read-only privileges, with the only exception of the QPR, where they can give feedback.
* Data validation mechanisms are in place to ensure the accuracy and consistency of salary and performance-related information.
* Regular audits and checks are conducted to identify and rectify any discrepancies or unauthorized alterations.
* An overwrite capability is limited to executives or those with approval, maintaining the integrity of the original data.
* Managers can request access after projections are approved, providing flexibility without compromising data integrity.

**Availability:**

* Redundancy and failover mechanisms are implemented to minimize downtime and ensure continuous availability of the system.
* An incident response plan is established to swiftly address and recover from any disruptions, ensuring minimal impact on availability.
* Contingency plans for power outages include a temporary UPS, ensuring system continuity.
* The server is mirrored to a nearby hot site, providing redundancy, and minimizing downtime.
* In anticipation of fires or natural disasters, relocation considerations have been made, with plans to move to a different state if necessary.
* Database mirroring at the Equinix Data Center in Chicago, Illinois, and backup services through Amazon Web Services add layers of availability, allowing users to access the system even in adverse conditions.

This integrated approach, in conjunction with the plan's pillars of confidentiality, integrity, and availability, fortifies the security framework, assuring the protection and seamless operation of the new salary and performance management system.

**Risk Management Assessment**

Assets are listed below and ranked according to their service importance:

| **Service** | **Confidentiality** | **Integrity** | **Availability** |
| --- | --- | --- | --- |
| Salary and Performance Management System | High | High | High |
| DBMS Server | High | High | High |
| HR Resources | Medium | Low | Medium |
| User ID and Credentials | High | Medium | Medium |
| Salary and Performance Procedures | High | Medium | Low |

Risk descriptions are described and ranked according to their impact on operations and the estimated vulnerability rating:

| **Risk ID** | **Risk Description** | **Example** | **Impact (1-10)** | **Vulnerability Score (1-10)** |
| --- | --- | --- | --- | --- |
| R1 | Unauthorized Access | Unauthorized individuals gaining access to sensitive data. | 8 | 7 |
| R2 | Data Loss | Loss or corruption of critical data due to system failure or cyberattack. | 9 | 6 |
| R3 | System Downtime | Extended periods of system unavailability due to technical issues. | 7 | 5 |
| R4 | Power Outages | Disruption of system operations due to power failures. | 6 | 4 |
| R5 | Natural Disasters | Impact of natural disasters like earthquakes or floods on system operations. | 9 | 8 |
| R6 | Insufficient User Training | Users lacking awareness of security best practices. | 5 | 3 |
| R7 | Third-Party Service Failures | Failures in services provided by external vendors. | 7 | 6 |
| R8 | Physical Theft | Theft of physical devices containing sensitive information. | 8 | 7 |

The following calculates a simple risk score based on previous factors:

| **Risk Description** | **Risk Score (1-100)** |
| --- | --- |
| Unauthorized Access | 85 |
| Data Loss | 70 |
| System Downtime | 60 |
| Power Outages | 50 |
| Natural Disasters | 75 |
| Insufficient User Training | 40 |
| Third-Party Service Failures | 65 |
| Physical Theft | 75 |

**Security Controls**

1. **Physical Security (Level 1):**
   * **Access Controls:** Physical access to servers and data centers hosting the system is restricted to top executives and technicians (if necessary).
   * **Security Measures:** Surveillance cameras, biometric access controls, and secure entry points are employed to protect physical assets.
2. **Network Security (Level 2):**
   * **Firewalls:** Robust firewalls are implemented to control and monitor traffic between the cloud-based system and external networks.
   * **Encryption:** Network traffic, especially sensitive data transmissions, is encrypted to prevent unauthorized interception.
3. **Application Security (Level 3):**
   * **Access Controls:** Role-based access controls are applied within the application to restrict user privileges.
   * **Secure Coding:** The application is developed with secure coding practices to prevent common vulnerabilities.
4. **File Security (Level 4):**
   * **Data Encryption:** Files containing sensitive information, such as salary and performance data, are encrypted to protect confidentiality.
   * **Access Controls:** File-level access controls are implemented to ensure only authorized users can access specific data files.
5. **Procedural Security (Level 5):**
   * **Security Policies:** Clear security policies are defined and communicated to all personnel accessing the system.
   * **Training:** Regular training programs ensure that employees understand and adhere to security procedures.
6. **User Security (Level 6):**
   * **Authentication:** Strong authentication mechanisms are implemented for user access, such as multi-factor authentication.
   * **User Education:** Users are educated about security best practices, emphasizing their role in maintaining a secure environment.

This security plan is a collaborative effort, with input from the security team, systems analysts, and tech leads involved in developing and maintaining the new Salary and Performance Management System.

This Security Plan follows the development lifecycle:

* Initiate the Security Plan during the design phase to align security measures with system architecture.
* Regularly review and update the plan as the system evolves.
* Validate that security controls effectively protect salary and performance data during testing.
* Finalize and implement security measures before the system goes live.

Regular reviews are crucial to adapting the plan to changing security landscapes and ensuring ongoing effectiveness in safeguarding sensitive employee information.

Our Security Plan for the new Salary and Performance Management System prioritizes strong safeguards at every level. From secure access controls and encryption protocols to comprehensive risk assessments, our approach ensures confidentiality, integrity, and availability of critical information. Key measures include a cloud-based environment with precise access controls and layered redundancy for uninterrupted system availability. Clear boundaries are set, focusing on essential elements within scope, while solid procedural and user-level security measures, such as multi-factor authentication, fortify our defense against potential threats. Our comprehensive security framework aligns with industry standards, emphasizing ongoing reviews to adapt to evolving landscapes and emerging risks.