**CY5200 Security Risk Management and Assessment**

**Module 9 Assignment**

**By: Kalp Shah**

**002232460**

**Note: Part I, III, IV is submitted in Excel submission link. (III and IV is combined)**

**l**

|  |  |
| --- | --- |
| **Asset1** | $1,000,000 |
| **Probability1** | 10% |
| **RiskImpact1** | 95% |
| **RiskofAsset1** | $95,000 |
| **RiskduetoVulnerability1** | $95,000 |

Assuming Threat T1 exploits Vulnerability V1 on Asset A1

Using Bayes Theorem,

**Probability(T1\*V1) =** 10%

**ProbabilityRI1 (RI1 | T1\*V1) =** 95%

**Probability(T1\*V1\*RI1) =** Probability(T1\*V1) \* ProbabilityRI1 (RI1 | T1\*V1) = 10% \* 95% = 9.5%

**Probability of a loss exceeding given values in $K**

|  |  |
| --- | --- |
| Probability(Loss>0) | 1 |
| Probability(Loss>50) | 0.4 |
| Probability(Loss>100) | 0.1 |

**Cumulative Distribution Function (CDF) in $K**

|  |  |
| --- | --- |
| CDF(Loss<=0) | 0 |
| CDF(0<Loss<=50) | 0.6 |
| CDF(50<Loss<=100) | 0.9 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Losses** | **Probality( Risk Loss |T1\*V1\*RI)** | **Probality( R1\*T1\*V1\*RI)** | **Sampling Ranges** |
| 0 | 0 | 90.5 | 0% to 90.5% |
| 0< Loss <= 50k | 60% | 5.7 | 90.5% to 96.20% |
| 0<Loss <= 100k | 30% | 2.85 | 96.20% to 99.05% |
| 0<Loss <= 200k | 10% | 0.95 | 99.05% to 100% |

**Calculation for Loss Excedeence**

|  |  |  |
| --- | --- | --- |
| **Risk Losses** | **Loss Exceedence Probability Function** | **Loss Exceedence Probability Sampling Ranges** |
| 0 | 100.00% | 100% |
| 0< Loss <= 50k | 9.50% | 9.50% to 3.8% |
| 0<Loss <= 100k | 3.80% | 3.80% 0.95% |
| 0<Loss <= 200k | 0.95% | 0.95% to 0.00% |

**Monte Carlo Simulation**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLOOKUP Table Array** | **Risk** | **Mote Carlo Rand()** | **Monte Carlo Values** | **Risk** |
| 0 | 0 | 6.377093604 | 29.79208896 | 0 |
| 91% | 50k | 46.47667409 | 86.68354318 | 0 |
| 96.20% | 100k | 99.66648696 | 46.12016345 | 200K |
| 99.05% | 200k | 81.98783924 | 14.19433872 | 0 |
|  |  | 90.89471185 | 16.91734409 | 50K |
|  |  | 86.391583 | 65.60943436 | 0 |
|  |  | 24.95066717 | 39.60135083 | 0 |
|  |  | 1.20788032 | 61.62288594 | 0 |
|  |  | 35.14212172 | 40.57836308 | 0 |
|  |  | 81.1469339 | 66.24180849 | 0 |
|  |  | 64.84528935 | 61.59362374 | 0 |

**II**

**Company Name –** Ayurhealthybaby

**Description –** Ayurhealthybaby is a health organization and clinic catering to the needs of customers regarding infertility problems. It contains 55 employees including doctors, staff, IT team, and management with presence in Gujarat, India and provides online services. It also has research development infrastructure that studies and creates different methods based on Garbhasanskar.

**Database Risk Management Implementation Plan**

**List of Cybersecurity controls**

**Authentication:**

1. Password Strength Policy – Implementation of strong password policies stating the length of the password and the mandatory inclusion of charset and symbols.
2. Multi-factor authentication – MFA enforcement ensures the authentication mechanism providing extra layer of security along with login credentials.
3. Monitoring – Continuous monitor the login attempts with the relevant user accounts and log the unusual and failed login incidents.
4. Review and Update: Review the password policies and make necessary changes according to the industry standards.
5. Biometric Authentication – Application of biometric authentication to add extra layer of security. It can include fingerprints, iris scan, etc.
6. Password Expiration Policies: Ensure password expiration policies are implemented requiring creating new and different password after a period of time.

**Authorization:**

1. Access Control – Define and implement access control policies according to the employee/user roles.
2. RBAC – Implement Role Based Access Control to manage and limit user permissions as required and efficiently.
3. Monitor and Review – Review and monitor access control policies in a timely manner according to the requirements.

**Confidentiality:**

1. Encryption – Encrypt the data at rest and in transit as per the industry standards.
2. Access Control – Implement access control to maintain confidentiality of the data on need-to-know basis.
3. Data deletion – Delete or dispose of the data and the information by performing known and reliable methods. Taking an example, DOD 3-way swipes is the common method followed.

**Data Integrity:**

1. Access Control – Implement access control to maintain integrity of the data to avoid any unauthorized access of the information and prevent tampering or manipulation.
2. Hashing and Digital Signatures – Enforce hashing and digital signatures to help verify the integrity of data.
3. Auditing – Perform audit procedures to track any changes made to the configurations or the data of the database.
4. Data Validation – Perform input data validation methods before storing the data into the database.

**Auditing:**

1. Log Protection – The logs should be protected using encryption and access control mechanisms from potential manipulation.
2. Review and Logging – Monitor the database changes and review it. Along, log the changes in the database.
3. Security Assessment – Perform security risk assessments in a timely manner to detect, mitigate, and forecast the database threats and vulnerabilities.
4. Alerts – Real time alerts should be in place to alert the administrator of the potential unwanted or suspicious activity or changes in the database.

**Replication and Federation:**

1. Data Replication - Data replication is an important measure to maintain copies of databases to help recover from data manipulation, disaster, and more.
2. Data Federation – Integration of the data from multiple database sources into one centralized database.
3. Encryption - Implementation of encryption to secure the copies of the data during data replication methods.
4. Data validation - Validate the data from the different sources during the data federation process.

**Clustering:**

1. Health Monitoring – Continuous monitoring the health of the database of each clustered database group.
2. Load balancing – Implement load balancing measures to divide the traffic and operations to the various nodes of the database and to perform efficiently.

**Backup and Recovery:**

1. Daily Backup – Perform daily backup of the database preventing from data loss in the case of disaster or more.
2. Encryption – Encrypt the backup data to maintain the confidentiality of the data.
3. Offsite Backup – The backup database should be in the offsite location to ensure its recovery in the case of disaster.

**Operating System Protection:**

1. Disk Partition – The disk partition for the database should be properly configured.
2. Updates and Patches – Regular updating the OS should be performed and the patches of the current OS should be installed.
3. Firewalls – Firewalls should be enforced on all the components and data of the OS and device.
4. Antivirus – Antivirus should be installed to protect the OS from compromising the data, device, and OS integrity, confidentiality, and availability.

**Application Protection:**

1. Secure Coding – Secure coding practices should be implemented while developing the database application.
2. Code Review – After the development of the application, the SAST should be performed during Ci/CD pipeline.
3. Security Risk Assessment – Risk assessment should be performed for the application with evolving threat landscape.
4. Regular Updates – Updates and patches should be installed of the application.

**Network Protection:**

1. VPN and Proxy – VPN and proxy should be installed and used to ensure the extra layer of protection and confidentiality.
2. Network Segmentation - Network Segmentation should be implemented to protect the critical databases parts from the external threats and exposure.
3. IDS/IPS – IDS/IPS systems should be implemented to monitor and alert the malicious activity towards the database.
4. SSL/TLS – Encryption networking protocols should be used to maintain the confidentiality of the data.

**Security Design and Configuration:**

1. Infrastructure security – Infrastructure security should be implemented to assess and maintain the health and security of the database ecosystem.
2. Secure Configuration – Configurations enforced in the database should be tested to check it’s working and effectiveness.
3. Compliance – Deploy the database system according to the industry standards and complying to the regulations and frameworks.
4. Security Risk Assessment – Risk assessment should be performed for the database design and configurations with evolving threat landscape.

**Enclave and Computing Environment:**

1. Secure configurations – Check the configurations of the enclaves and test periodically.
2. Access Control – Access controls should be implemented to enforce authorization practices.
3. Physical security – Physical security of enclaves and databases should be ensured.
4. IDS/IPS – Enhanced and stealth modes of IDS/IPS should be activated.

**Business Continuity:**

1. Business Continuity Plan - Business Continuity plans should be devised and enforced during the downtime of the systems.
2. Testing – The business continuity plan should be tested, and drills be performed to check its effectiveness.
3. Review and Update – The business continuity plan should be reviewed periodically and updated according to the changing infrastructure of the organization and evolving threat landscape.
4. Offsite Redundant Backup – The backup database should be in the offsite location to ensure its recovery in the case of disaster.

**Vulnerability and Incident Management:**

1. Vulnerability and Security Risk Assessment – Periodic assessment for the new vulnerabilities or threats should be undertaken.
2. Threat Intelligence – Staying updated with the evolving threat landscape to overcome and secure the database.
3. SOC and Incident Response – SOC and incident response teams should be hired to monitor and act on the threats and risks acting upon the organization.

**Network Topology of Ayurhealthybaby**

**A diagram of a network

Description automatically generated**

The above image represent the topology of Ayurhealthybaby. Here the PC(s), printers and CCTV(s) are connected to the router. The router is connected to the internet as is defended by firewall. Additionally, the server and database of Ayurhealthybaby is also connected to the router. Moreover, VPN is established to provide encryption, authentication, and encapsulation for the communications.

**List of all Network Risk Management Implementation controls at Ayurhealthybaby**

**Authentication:**

1. Password Strength Policy – Implementation of strong password policies stating the length of the password and the mandatory inclusion of charset and symbols.
2. Multi-factor authentication – MFA enforcement ensures the authentication mechanism providing extra layer of security along with login credentials.
3. Monitoring – Continuous monitor the login attempts with the relevant user accounts and log the unusual and failed login incidents.
4. Review and Update: Review the password policies and make necessary changes according to the industry standards.
5. Password Expiration Policies: Ensure password expiration policies are implemented requiring creating new and different password after a period of time.

**Authorization:**

1. Access Control – Define and implement access control policies according to the employee/user roles.
2. RBAC – Implement Role Based Access Control to manage and limit user permissions as required and efficiently.

**Confidentiality:**

1. Encryption – Encrypt the data at rest and in transit as per the industry standards.
2. Access Control – Implement access control to maintain confidentiality of the data on need-to-know basis.

**Data Integrity:**

1. Access Control – Implement access control to maintain integrity of the data to avoid any unauthorized access of the information and prevent tampering or manipulation.
2. Auditing – Perform audit procedures to track any changes made to the configurations or the data of the database.
3. Data Validation – Perform input data validation methods before storing the data into the database.

**Auditing:**

1. Log Protection – The logs should be protected using encryption and access control mechanisms from potential manipulation.
2. Review and Logging – Monitor the database changes and review it. Along, log the changes in the database.
3. Alerts – Real time alerts should be in place to alert the administrator of the potential unwanted or suspicious activity or changes in the database.

**Replication and Federation:**

1. Data Replication - Data replication is an important measure to maintain copies of databases to help recover from data manipulation, disaster, and more.
2. Data Federation – Integration of the data from multiple database sources into one centralized database.
3. Encryption - Implementation of encryption to secure the copies of the data during data replication methods.
4. Data validation - Validate the data from the different sources during the data federation process.

**Clustering:**

1. Health Monitoring – Continuous monitoring the health of the database of each clustered database group.

**Backup and Recovery:**

1. Daily Backup – Perform daily backup of the database preventing from data loss in the case of disaster or more.
2. Encryption – Encrypt the backup data to maintain the confidentiality of the data.
3. Offsite Backup – The backup database should be in the offsite location to ensure its recovery in the case of disaster.

**Operating System Protection:**

1. Updates and Patches – Regular updating the OS should be performed and the patches of the current OS should be installed.
2. Firewalls – Firewalls should be enforced on all the components and data of the OS and device.
3. Antivirus – Antivirus should be installed to protect the OS from compromising the data, device, and OS integrity, confidentiality, and availability.

**Application Protection:**

1. Secure Coding – Secure coding practices should be implemented while developing the database application.
2. Regular Updates – Updates and patches should be installed on the application.

**Network Protection:**

1. VPN and Proxy – VPN and proxy should be installed and used to ensure the extra layer of protection and confidentiality.
2. SSL/TLS – Encryption networking protocols should be used to maintain the confidentiality of the data.

**Security Design and Configuration:**

1. Secure Configuration – Configurations enforced in the database should be tested to check it’s working and effectiveness.
2. Compliance – Deploy the database system according to the industry standards and complying to the regulations and frameworks.

**Enclave and Computing Environment:**

1. Secure configurations – Check the configurations of the enclaves and test periodically.
2. Access Control – Access controls should be implemented to enforce authorization practices.
3. Physical security – Physical security of enclaves and databases should be ensured.

**Business Continuity:**

1. Business Continuity Plan - Business Continuity plans should be devised and enforced during the downtime of the systems.
2. Testing – The business continuity plan should be tested, and drills be performed to check its effectiveness.
3. Offsite Redundant Backup – The backup database should be in the offsite location to ensure its recovery in the case of disaster.

**Vulnerability and Incident Management:**

1. Threat Intelligence – Staying updated with the evolving threat landscape to overcome and secure the database.

**List of all Network Risk Management Implementation PRESENT/ABSENT controls at Ayurhealthybaby**

|  |  |
| --- | --- |
| **Controls** | **Status** |
| **Authentication** | |
| Password Strength Policy | Present |
| Multi-factor authentication | Present |
| Monitoring | Present |
| Review and Update | Present |
| Biometric Authentication | Absent |
| Password Expiration Policies | Present |
| **Authorization** | |
| Access Control | Present |
| RBAC | Present |
| Monitor and Review | Absent |
| **Confidentiality** | |
| Encryption | Present |
| Access Control | Present |
| Data deletion | Absent |
| **Data Integrity** | |
| Access Control | Present |
| Hashing and Digital Signatures | Absent |
| Auditing | Present |
| Data Validation | Present |
| **Auditing** | |
| Log Protection | Present |
| Review and Logging | Present |
| Security Assessment | Absent |
| Alerts | Present |
| **Replication and Federation** | |
| Data Replication | Present |
| Data Federation | Present |
| Encryption | Present |
| Data validation | Present |
| **Clustering** | |
| Health Monitoring | Present |
| Load balancing | Absent |
| **Backup and Recovery** | |
| Daily Backup | Present |
| Encryption | Present |
| Offsite Backup | Present |
| **Operating System Protection** | |
| Disk Partition | Absent |
| Updates and Patches | Present |
| Firewalls | Present |
| Antivirus | Present |
| **Application Protection** | |
| Secure Coding | Present |
| Code Review | Absent |
| Security Risk Assessment | Absent |
| Regular Updates | Present |
| **Network Protection** | |
| VPN and Proxy | Present |
| Network Segmentation | Absent |
| IDS/IPS | Absent |
| SSL/TLS | Present |
| **Security Design and Configuration** | |
| Infrastructure Security | Absent |
| Secure Configurations | Present |
| Compliance | Present |
| Security Risk Assessment | Absent |
| **Enclave and Computing Environment** | |
| Secure Configurations | Present |
| Access Control | Present |
| Physical Security | Present |
| IDS/IPS | Absent |
| **Business Continuity** | |
| Business Continuity Plan | Present |
| Testing | Present |
| Review and Update | Absent |
| Offsite Redundant Backup | Present |
| **Vulnerability and Incident Management** | |
| Vulnerability and Security Risk Assessment | Absent |
| Threat Intelligence | Present |
| SOC and Incident Response | Absent |

**Critical Assets List in $ that exist in Ayurhealthybaby:**

|  |  |  |
| --- | --- | --- |
| Asset Number | Asset Name | Value |
| A1 | Sensitive Documents | 100,000 |
| A2 | Personnel Information | 20,000 |
| A3 | Financial Documents | 10,000 |
| A4 | Server | 5,000 |
| A5 | Network Services and Database | 50,000 |
| A6 | CCTV Hardware and Server | 2,000 |
| A7 | PCs | 7,000 |
| A8 | Printers | 1,000 |
| A9 | Reputation | Intangible |
| A10 | Clinical Materials and Hardware | 70,000 |

**List of Potential Vulnerabilities for critical assets where cybersecurity Implementation Controls are missing**

|  |  |
| --- | --- |
| Missing Controls | Vulnerabilities |
| **Authentication** | |
| Biometric Authentication | Lack of Authentication, Unauthorized Access |
| **Authorization** | |
| Monitor and Review | Unauthorized Access, Data Exfiltration |
| **Confidentiality** | |
| Data Deletion | Information Disclosure |
| **Data Integrity** | |
| Hashing and Digital Signature | Data Tampering, Lack of Compliance, Data Repudiation |
| **Auditing** | |
| Security Risk Assessment | Ineffective Log Analysis, Weak Audit Trail Protection |
| **Clustering** | |
| Load Balancing | Data Leakage, Inadequate Monitoring and Logging, Single Point of Failure |
| **Operating System Protection** | |
| Disk Partition | Lack of Access Control, Lack of Encrypted Boot Partition |
| **Application Protection** | |
| Code Review | Injection, XSS, Broken Access Control, CSRF, IDOR |
| Security Risk Assessment | Ineffective Risk Management and Mitigation |
| **Network Protection** | |
| Network Segmentation | Inadequate Monitoring, Data Exfiltration |
| IDS/IPS | IP address spoofing, Weak Signature Detection |
| **Security Design and Configuration** | |
| Infrastructure Security | Lack of Authentication, Security Misconfigurations, Lack of Access Control |
| Security Risk Assessment | Ineffective Risk Management and Mitigation, Lack of vulnerability assessment and tracking |
| **Enclave and Computing Environment** | |
| IDS/IPS | IP address spoofing, Weak Signature Detection |
| **Business Continuity** | |
| Review and Update | Outdated Documentation, Lack of Risk Assessment, Single Point of Failure |
| **Vulnerability and Incident Management** | |
| Vulnerability and Security Risk Assessment | Lack of vulnerability assessment and tracking |
| SOC and Incident Response | Lack of Incident Response, Interruption of Operations, Lack of Monitoring and Logging |

**List of Potential Vulnerabilities:**

1. Unauthenticated/Unauthorized Access
2. Poor security policies and compliance
3. Lack of encryption implementation
4. Inadequate access-control
5. Lack of monitoring and logging
6. IP address spoofing
7. Data Repudiation
8. Lack of vulnerability assessment and tracking
9. Lack of Incident Response
10. Single Point of Failure
11. Outdated Documentation
12. Weak Signature Detection
13. Ineffective Risk Management and Mitigation
14. Security Misconfigurations
15. Data Exfiltration / Data Leakage
16. Injection
17. XSS
18. CSRF
19. IDOR
20. Weak Audit Trail Protection

**List of Potential threats on Critical Assets:**

|  |  |
| --- | --- |
| **Assets** | **Threat** |
| Sensitive Documents | Disclosure of Information, data breach, data theft |
| Personnel Information | Disclosure of Information, data breach, data theft |
| Financial Documents | Disclosure of Information, data breach, data theft |
| Server | Denial of Service, Malware, Interruption of operations |
| Network Services and Database | Denial of Service, Malware, Interruption of operations |
| CCTV Hardware and Server | Denial of Service, Malware, Interruption of operations |
| PCs | Malware, Disclosure of Information |
| Printers | Interruption of operations |
| Reputation | Disclosure of Information, data breach, data theft, Market loss |
| Clinical Materials and Hardware | Interruption of operations |

**List of potential threats**

1. Disclosure of Information
2. Information theft and breach
3. Denial of Service – DoS/DDoS
4. Malware and virus
5. Interruption of Operations
6. Man-in-the-middle attack
7. IP address hijacking
8. Eavesdropping

**List of Potential Risks for Critical Assets Due to Missing Controls:**

|  |  |
| --- | --- |
| Missing Controls | Risk |
| **Authentication** | |
| Biometric Authentication | Unauthorized access, Information Disclosure and data breach, Disgruntled employee |
| **Authorization** | |
| Monitor and Review | Unauthorized access, Information Disclosure and data breach, Disgruntled employee |
| **Confidentiality** | |
| Data Deletion | Information Disclosure and data breach, Disgruntled employee |
| **Data Integrity** | |
| Hashing and Digital Signature | Unauthorized access |
| **Auditing** | |
| Security Risk Assessment | Prone to malware and virus attacks, Interruption in operations |
| **Clustering** | |
| Load Balancing | Compromise of network, Interruption in operations |
| **Operating System Protection** | |
| Disk Partition | Information Disclosure and data breach |
| **Application Protection** | |
| Code Review | Interruption in operations |
| Security Risk Assessment | Prone to malware and virus attacks, Interruption in operations |
| **Network Protection** | |
| Network Segmentation | Interruption in operations |
| IDS/IPS | Unauthorized access, Interruption in operations |
| **Security Design and Configuration** | |
| Infrastructure Security | Interruption in operations |
| Security Risk Assessment | Prone to malware and virus attacks |
| **Enclave and Computing Environment** | |
| IDS/IPS | Prone to malware and virus attacks, Unauthorized access, Compromise of network, Interruption in operations |
| **Business Continuity** | |
| Review and Update | Interruption in operations |
| **Vulnerability and Incident Management** | |
| Vulnerability and Security Risk Assessment | Prone to malware and virus attacks, Unauthorized access, Interruption in operations |
| SOC and Incident Response | Prone to malware and virus attacks, Compromise of network, Interruption in operations |

**List of Potential Risks due to missing Cybersecurity Implementation Controls:**

1. Unauthorized access.
2. Prone to malware and virus attacks.
3. Interruption in operations.
4. Information Disclosure and data breach.
5. Compromise of network.
6. Disgruntled employee.

**List of recommended policies for each security control as a part of risk prevention strategy**

**Authentication:**

* Lock the account after a certain number of failed login attempts.
* Strengthen password policies from time to time and implement it stringent manner.
* Enforce biometric authentication in place along with passwords to add extra layer of security.

**Authorization:**

* Continuously monitor and review logs of the authorization and authentication attempts.
* Implement strict access control with least privilege access model and avoiding any misconfigurations.

**Confidentiality:**

* Enforce data masking policies making sensitive and confidential information secure and resulting in obfuscation in exposed or non-isolated environment.
* Perform DOD 3 swipe method to make sure the discarded devices or deleted content cannot be retrieved.

**Data Integrity:**

* Implement data validation policies including hashing and digital signatures to ensure the accuracy and consistency.

**Auditing:**

* Perform regular security risk assessment.
* Implement effective log analysis measures and methods.
* Audit trails should be protected to prevent from data manipulation.

**Replication and Federation:**

* Physical security should be ensured of the offsite databases.
* Encryption methods should meet the industry standards and compliance regulations.

**Clustering:**

* Implement load balancing techniques and nodes to prevent single point of failure and data leakage.

**Backup and Recovery:**

* Physical security should be ensured of the offsite databases.
* Encryption methods should meet the industry standards and compliance regulations.
* Implement Recovery Time Objective(RTO) and Recovery Point Objective(RPO) policies.

**Operating System Protection:**

* Implement patch management policy to timely update and patch the versions of OS.
* Ensure the disk partition according to the data confidentiality and impose access controls and encryption modules accordingly.

**Application Protection:**

* Secure coding practices should be implemented along with the code review and risk assessment to prevent injection, XSS, CSRF, etc. vulnerabilities.

**Network Protection:**

* Network Segmentation should be applied to improve categorical and effective monitoring and prevent data exfiltration.
* Firewall policies should be stringent and on stealth mode when required.
* DMZ implementation along with effective monitoring.

**Security Design and Configuration:**

* As per industry standards, compliance and best practices implement secure design principles.

**Enclave and Computing Environment:**

* Physical security should be ensured of the offsite databases.
* Encryption methods should meet the industry standards and compliance regulations.
* Perform security risk assessment and avoiding security misconfigurations.

**Business Continuity:**

* Test the business continuity plan to discover any loopholes or missing measures.
* Train the employees to avoid any mishaps during actual implementations

**Vulnerability and Incident Management:**

* Dedicated SOC center and Incident response team should be hired for continuous monitoring, logging and taking actions.

**List of recommended policies for each security control as a part of risk resilience/response strategy**

**Authentication:**

* Lock the affected accounts and revoke all privileges and permissions of the user account.
* Change the user account passwords.

**Authorization:**

* Revoke access control permissions of the affected user’s account.

**Confidentiality:**

* Change the encryption keys and passphrases to ensure the confidentiality is intact.

**Data Integrity:**

* Regenerate hashes and digital signatures of the system data and database.

**Replication and Federation:**

* Actively scan for malware and viruses in the system for the offsite databases.
* Change the encryption keys and passphrases to ensure the confidentiality is intact.

**Clustering:**

* Rollback to the previous configurations to nullify the malicious configuration changes.

**Backup and Recovery:**

* Create a secure redundant database storage, servers, and networking channels to make it active in cases of shut down or interruption of previous deployed services.

**Operating System Protection:**

* Actively scan for malware and viruses in the system.
* Change the user account passwords.

**Application Protection:**

* Enable firewall on application level.

**Network Protection:**

* Redirect traffic to the redundant infrastructure and isolate the affected system.
* Shift firewalls to stealth mode for enhanced surveillance and logging.
* Implement malware and virus detection procedures in depth.
* Modify the firewall rules according to an attack.

**Security Design and Configuration:**

* Rollback to the previous security configurations to nullify the malicious configuration changes.
* Harden the security configuration and restrict the communication and protocol access as required.

**Enclave and Computing Environment:**

* Create and establish incident response plan.
* Make strategy and implement for data recovery from the previous backup.
* Isolate the affected infrastructure to ensure least interruptions in operations.

**Business Continuity:**

* Implement business continuity plan and enable proactive measures to overcome the attack effects.
* Have appropriate cyber insurance according to the company’s requirement to cover the financial costs of the losses caused by an attack.

**Vulnerability and Incident Management:**

* Monitor and alert the incident response team and the appropriate stakeholders.
* Implement IR Plan policies and provide periodic reports to C-suite personnels.

**Database Credentials Coding Policy**

# 1. Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

# 2. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Ayurhealthybaby's networks.

Software applications running on Ayurhealthybaby's networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

# 3. Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the Ayurhealthybaby Network. This policy applies to all software (programs, modules, libraries or APIS that will access a Ayurhealthybaby, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don’t always use sanitized information.

# 4. Policy

In order to maintain the security of Ayurhealthybaby's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

Specific Requirements

Storage of Data Base User Names and Passwords

* Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
* Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
* Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
* Database credentials may not reside in the documents tree of a web server.
* Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
* Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

Retrieval of Database User Names and Passwords

* If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

* The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

* For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

Access to Database User Names and Passwords

* Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
* Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
* Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

# 5. Policy Compliance

5.1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.2. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Ayurhealthybaby.

Any program code or application that is found to violate this policy must be remediated within a 90 day period.

# 6. Related Standards, Policies and Processes

• Password Policy

# 7. Definitions and Terms

* Credentials
* Executing Body
* Hash Function
* LDAP
* Module

# 8. Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| September 2023 | Kalp Shah | V1.0 = Password policy has been introduced |