**CY5200 Security Risk Management and Assessment**

**Module 5 Assignment**

**By: Kalp Shah**

**002232460**

**Note: Excel spreadsheet for Part 1 and 3 are attached in the excel submission link.**

**I**

**Verification of error estimation formula:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| P | z | Confidence Level | 1200 | 1400 | 1600 | 1800 | 4000 |
| 0.5 | 2.575829304 | 0.99 | 3.717889354 | 3.442097 | 3.219787 | 3.035644 | 2.036372 |
| 0.5 | 1.959963985 | 0.95 | 2.828964335 | 2.619112 | 2.449955 | 2.30984 | 1.549488 |
| 0.5 | 1.644853627 | 0.9 | 2.374141711 | 2.198028 | 2.056067 | 1.938479 | 1.300371 |

**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.

**List of all Cyber Security Implementation controls**

**Identification Credentials:**

**PIN –** A numeric sequence used for personal authentication along with identification of employee.

**Password –** A alphanumeric charset sequence used for same purpose as of PIN and provides authentication.

**Digital Signature –** Provides non-repudiation along with authentication in a a cryptographic manner attaching transaction details and entities involved in it.

**ID Card –** Identifies the person along with the photo and basic details helping to confirm the person’s identity and prevent unauthorized access physically.

**Biometrics –** Additional layer of authentication with advanced identification system and less chances of duplication thwarting cases of identity theft.

**Smart Cards –** A card embedded with chip ensuring the access of the premises to the card holder.

**Aadhar Card –** Government issues ID identifying person and verifying his/her details along with photograph.

**PKI –** The ecosystem of public and private key authentication used to verify users identity and authorization.

**Personal Authentication:**

**PIN -** A numeric sequence used for personal authentication along with identification of employee.

**Password –** A alphanumeric charset sequence used for same purpose as of PIN and provides authentication.

**ID Card–** Identifies the person along with the photo and basic details helping to confirm the person’s identity and prevent unauthorized access physically.

**Biometrics –** Additional layer of authentication with advanced identification system and less chances of duplication thwarting cases of identity theft.

**Smart Cards –** A card embedded with chip ensuring the access of the premises to the card holder

**Aadhar Cards–** Government issues ID identifying person and verifying his/her details along with photograph.

**Private Key -** A cryptographic key kept confidential and known only to the individual or entity it belongs to.

**Multi Factor Authentication -** Multiple forms of identification, such as passwords, biometrics, or security tokens, to access a system or account.

**Authorization:**

**Access Control List -** A list of rules that define permissions and restrictions for users accessing resources.

**Security Tokens -** Physical or digital devices that generate one-time passwords or codes to enhance user authentication

**Security Policy –** A set of rules, recommendations, and guidelines for securing company’s assets and be complaint with the federal frameworks and standards

**Least Privilege Principle -** The minimum level of access or permissions necessary to perform their tasks, reducing the risk of unauthorized actions

**Logical Access Control:**

**Network Architecture Controls -** Configurations implemented to mitigate security risks and control access, often involving firewalls, routers, and IDS/IPS.

**Remote Network Access -** Connecting to a network from an external location, requiring secure protocols and authentication mechanisms.

**Secure Network Ports -** Network ports that adhere to security protocols and policies, reducing the risk of unauthorized access or data breaches.

**Port Authentication using 802.1x -** Access control method that requires devices to authenticate before being granted access to a network

**Network Access Control (NAC) system –** Thesystem that manages and implements security policies before allowing devices to connect to a network.

**Encryption –** The mechanism to convert the readable data to secure code that requires key or passphrase to decode.

**Password –** A alphanumeric charset sequence used for same purpose as of PIN and provides authentication.

**PIN -** A numeric sequence used for personal authentication along with identification of employee.

**Physical Access Control:**

**Classified Database –** Secure encrypted database ensuring confidentiality, integrity, and availability.

**Badges–** Identifies the person along with the photo and basic details helping to confirm the person’s identity and prevent unauthorized access physically.

**Smart Cards–** A card embedded with chip ensuring the access of the premises to the card holder.

**PIN -** A numeric sequence used for personal authentication along with identification of employee.

**Passwords –** A alphanumeric charset sequence used for same purpose as of PIN and provides authentication.

**Physical Tokens -** Devices, such as smart cards or USB tokens, used for authentication to enhance security.

**Aadhar Card–** Government issues ID identifying person and verifying his/her details along with photograph.

**Attended Access–** Physical security of the premises along with CCTV surveillance.

**Biometric Systems:**

**Retina Scan –** Iris scan to access the premises ensuring authentication and authorization.

**Fingerprint –** Fingerprint scan to access the premises ensuring authentication and authorization.

**Face ID –** Scanning of face to access the premises ensuring authentication and authorization.

**List of all Cyber Security Implementation controls at Ayurhealthybaby**

**Identification Credentials:**

**PIN -** A numeric sequence used for personal authentication along with identification of employee.

**Password –** A alphanumeric charset sequence used for same purpose as of PIN and provides authentication.

**ID Card–** Identifies the person along with the photo and basic details helping to confirm the person’s identity and prevent unauthorized access physically.

**Smart Cards- –** A card embedded with chip ensuring the access of the premises to the card holder.

**Personal Authentication:**

**PIN -** A numeric sequence used for personal authentication along with identification of employee.

**Password –** A alphanumeric charset sequence used for same purpose as of PIN and provides authentication.

**ID Card–** Identifies the person along with the photo and basic details helping to confirm the person’s identity and prevent unauthorized access physically.

**Smart Cards–** A card embedded with chip ensuring the access of the premises to the card holder.

**Multi Factor Authentication** - Multiple forms of identification, such as passwords, biometrics, or security tokens, to access a system or account.

**Authorization:**

**Access Control List-** A list of rules that define permissions and restrictions for users accessing resources.

**Logical Access Control:**

**Network Architecture Controls -** Configurations implemented to mitigate security risks and control access, often involving firewalls, routers, and IDS/IPS.

**Secure Network Ports -** Network ports that adhere to security protocols and policies, reducing the risk of unauthorized access or data breaches.

**Port Authentication using 802.1x -** Access control method that requires devices to authenticate before being granted access to a network

**Network Access Control (NAC) system –** Thesystem that manages and implements security policies before allowing devices to connect to a network.

**Password –** A alphanumeric charset sequence used for same purpose as of PIN and provides authentication.

**PIN -** A numeric sequence used for personal authentication along with identification of employee.

**Physical Access Control:**

**Badges / ID Card–** Identifies the person along with the photo and basic details helping to confirm the person’s identity and prevent unauthorized access physically.

**Smart Cards–** A card embedded with chip ensuring the access of the premises to the card holder.

**PIN -** A numeric sequence used for personal authentication along with identification of employee.

**Passwords –** A alphanumeric charset sequence used for same purpose as of PIN and provides authentication.

**Attended Access –** Physical security of the premises along with CCTV surveillance.

**List of all Cyber Security Implementation PRESENT/ABSENT controls at Ayurhealthybaby**

|  |  |
| --- | --- |
| Control | Status |
| **Identification Credentials** | |
| PIN | Present |
| Password | Present |
| Digital Signature | Absent |
| ID Card | Present |
| Biometrics | Absent |
| Smart Cards | Present |
| Aadhar Card | Absent |
| PKI | Absent |
| **Personal Authentication** | |
| PIN | Present |
| Password | Present |
| ID Card | Present |
| Biometrics | Absent |
| Smart Cards | Present |
| Aadhar Cards | Absent |
| Private Key | Absent |
| Multi Factor Authentication | Present |
| **Authorization** | |
| Access Control List | Present |
| Security Tokens | Absent |
| Security Policy | Absent |
| Least Privilege Principle | Absent |
| **Logical Access Control Methods** | |
| Network Architecture Controls | Present |
| Remote Network Access | Absent |
| Secure Network Ports | Present |
| Port Authentication using 802.1x | Present |
| Network Access Control (NAC) system | Present |
| Encryption | Absent |
| Password | Present |
| PIN | Present |
| **Physical Access Control Methods** | |
| Classified Database | Absent |
| Badges | Present |
| Smart Cards | Present |
| PIN | Present |
| Passwords | Present |
| Physical Tokens | Absent |
| Aadhar Card | Absent |
| Attended Access | Present |
| **Biometric Systems** | |
| Retina Scan | Absent |
| Fingerprint | Absent |
| Face ID | 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/Not Fully Present Controls** | **Vulnerability** |
| **Identification Credentials** | |
| Digital Signature | Lack of Identification controls, unauthorized access |
| Biometrics | Lack of Identification controls, unauthorized access |
| Aadhar Cards | Lack of Identification controls, unauthorized access |
| PKI | Lack of Identification, unauthorized access controls |
| **Personal Authentication** | |
| Biometrics | Lack of Authentication controls, unauthorized access |
| Aadhar Cards | Lack of Authentication controls, unauthorized access |
| Private Key | Lack of Authentication controls, unauthorized access |
| **Authorization** | |
| Security Tokens | Inadequate access control, unauthorized access, poor security policies |
| Security Policy | Inadequate access control, unauthorized access, poor security policies |
| Least Privilege Principle | Inadequate access control, unauthorized access, poor security policies |
| **Logical Access Controls** | |
| Remote Network Access | Weak network security, Inadequate access control |
| Encryption | Weak network security, Inadequate access control, theft, eavesdropping |
| **Physical Access Controls** | |
| Classified Database | Lack of physical security, theft |
| Physical Tokens | Lack of physical security, Lack of authentication |
| Aadhar Card | Lack of physical security, Lack of authentication |
| **Biometric Systems** | |
| Retina Scan | Lack of physical security, Lack of authentication, Inadequate access control |
| Fingerprint | Lack of physical security, Lack of authentication, Inadequate access control |
| Face ID | Lack of physical security, Lack of authentication, Inadequate access control |

**List of Potential Vulnerabilities:**

1. Lack of identification and authentication controls
2. Unauthorized access
3. Lack of physical security
4. Information theft and breach
5. Weak network security
6. Poor security policies and compliance

**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, Natural Disaster |
| Network Services and Database | Denial of Service, Malware, Interruption of operations, Natural Disaster |
| CCTV Hardware and Server | Denial of Service, Malware, Interruption of operations, Natural Disaster |
| PCs | Malware, Natural Disaster, Impostor |
| Printers | Interruption of operations, Natural Disaster |
| Reputation | Disclosure of Information, data breach, data theft, Market loss |
| Clinical Materials and Hardware | Physical theft, Natural disaster |

**List of potential threats**

1. Disclosure of Information
2. Information theft and breach
3. Denial of Service
4. Malware and virus
5. Interruption of Operations
6. Natural Disaster
7. Impostor and physical theft

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

|  |  |
| --- | --- |
| **Missing/Not Fully Present Controls** | **Risk** |
| **Identification Credentials** | |
| Digital Signature | Unauthorized access to the infrastructure |
| Biometrics | Unauthorized access to the infrastructure |
| Aadhar Cards | Unauthorized access to the infrastructure |
| PKI | Unauthorized access to the infrastructure |
| **Personal Authentication** | |
| Biometrics | Compromising user authentication |
| Aadhar Cards | Compromising user authentication |
| Private Key | Compromising user authentication |
| **Authorization** | |
| Security Tokens | Disclosure of information and breach of confidentiality and integrity |
| Security Policy | Disclosure of information and breach of confidentiality and integrity |
| Least Privilege Principle | Disclosure of information and breach of confidentiality and integrity |
| **Logical Access Controls** | |
| Remote Network Access | Compromising availability and business continuity |
| Encryption | Leads to violation of confidentiality |
| **Physical Access Controls** | |
| Classified Database | Compromise of confidentiality, information theft and unauthorized access |
| Physical Tokens | Unauthorized access to the infrastructure, compromising user authentication |
| Aadhar Card | Unauthorized access to the infrastructure, compromising user authentication |
| **Biometric Systems** | |
| Retina Scan | Unauthorized access to the infrastructure, compromising user authentication, information disclosure, lack of access control |
| Fingerprint | Unauthorized access to the infrastructure, compromising user authentication, information disclosure, lack of access control |
| Face ID | Unauthorized access to the infrastructure, compromising user authentication, information disclosure, lack of access control |

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

1. Unauthorized access to the infrastructure and facilities.
2. Compromise of confidentiality, integrity, and availability.
3. Compromise of user authentication.
4. Information Disclosure and data breach.
5. Identity theft.

**Remote Access Policy**

# **Overview**

Remote access to our corporate network is essential to maintain our Team’s productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Ayurhealthybaby policy, we must mitigate these external risks the best of our ability.

# **Purpose**

The purpose of this policy is to define rules and requirements for connecting to Ayurhealthybaby 's network from any host. These rules and requirements are designed to minimize the potential exposure to Ayurhealthybaby from damages which may result from unauthorized use of Ayurhealthybaby resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Ayurhealthybaby internal systems, and fines or other financial liabilities incurred as a result of those losses.

# **Scope**

This policy applies to all Ayurhealthybaby employees, contractors, vendors and agents with a Ayurhealthybaby-owned or personally-owned computer or workstation used to connect to the Ayurhealthybaby network. This policy applies to remote access connections used to do work on behalf of Ayurhealthybaby, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Ayurhealthybaby networks.

# **Policy**

It is the responsibility of Ayurhealthybaby employees, contractors, vendors and agents with remote access privileges to Ayurhealthybaby's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Ayurhealthybaby.

General access to the Internet for recreational use through the Ayurhealthybaby network is strictly limited to Ayurhealthybaby employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the Ayurhealthybaby network from a personal computer, Authorized Users are responsible for preventing access to any Ayurhealthybaby computer resources or data by non-Authorized Users. Performance of illegal activities through the Ayurhealthybaby network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the Acceptable Use Policy.

Authorized Users will not use Ayurhealthybaby networks to access the Internet for outside business interests.

For additional information regarding Ayurhealthybaby's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (company url).

* 1. **Requirements** 
     1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Acceptable Encryption Policy and the Password Policy.
     2. Authorized Users shall protect their login and password, even from family members.
     3. While using a Ayurhealthybaby-owned computer to remotely connect to Ayurhealthybaby's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
     4. Use of external resources to conduct Ayurhealthybaby business must be approved in advance by InfoSec and the appropriate business unit manager.
     5. All hosts that are connected to Ayurhealthybaby internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.
     6. Personal equipment used to connect to Ayurhealthybaby's networks must meet the requirements of Ayurhealthybaby-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to Ayurhealthybaby Networks.

# **Policy Compliance**

* 1. **Compliance Measurement**

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

# **Exceptions**

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

# **Non-Compliance**

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

# **Related Standards, Policies and Processes**

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Ayurhealthybaby’s network:

* Acceptable Encryption Policy
* Acceptable Use Policy
* Password Policy
* Third Party Agreement
* Hardware and Software Configuration Standards for Remote Access to Ayurhealthybaby Networks

# **Revision History**

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
| August 2021 | Kalp Shah | V 1.0 Updated policy on use of external resources |
| December 2022 | Kalp Shah | V 1.1 Updated non-compliance under policy compliance. |

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

1. Access Control: Improve and implement rigorous and strict controls restricting access to the authorized users to avoid information disclosure, theft, breach, and identity theft. Adding adhaar card, physical tokens, and PKi increases the access control standards.
2. Database and Encryption: Encrypt the stored the data to restrict information disclosure in crucial breaches. Additionally, encrypt the communication channels to avoid eavesdropping.
3. Network Monitoring and Security: Implement IAM and network monitoring tools that cover every communication channels and ports to secure it. Continuous log every activity and audit it periodically.
4. Awareness and Security Training: Hold periodic awareness sessions and training promoting infrastructure’s security to personnels and staff.
5. Backup and Update: Take regular backup of the system in the event of data loss or disaster. Along with, keep the tools and services updated to cover the vulnerability gap and attain patch management.
6. Simulations: Create blue/red teams and implement various scenarios of attacks based on subjective and objective data. Test the defenses and improve where it is lacking.

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

1. Incident Response: Implement SIEM and monitoring ecosystems. Prepare alerts and plans in case of an attack defining how to manage and mitigate it.
2. Business Continuity Plan: Create a plan to ensure the flow of the business with zero impact in the public during times of an attack.
3. Cyber Insurance: Have appropriate cyber insurance according to the company’s requirement to cover the financial costs of the losses caused by an attack.
4. Redundancy – 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.