

## APPENDIX A INTERVIEW PROTOCOL AND QUESTIONNAIRE

### 1. Research Overview

The following interview protocol was used to support the risk identification process in the field of Information and Communication Technology (ICT) at Agen Informasi Komunikasi dan Teknologi (TIC Timor IP), specifically within the Human Resources Division.

### 2. Respondent Information

Name :

Position :

Agency :

Length of service :

Day, Date :

### 3. Questionnaire Link

The questionnaire used in this study was distributed using an online platform and can be accessed through the following link:

<https://forms.gle/y5rxUq4p821XrppQ8>

<https://docs.google.com/spreadsheets/d/1fk48usB5bGdEIEuzCeMt-4NEyNqNSYI-w7Ran0BbE-w/edit?usp=sharing>

docs.google.com/forms/d/1R-otLjHRqTJHRnD-tKGAMdZyEEQcRiOHUMxAcRs/edit#responses

Untitled form

Questions Responses 2 Settings

6. Oinsa prosedimentu ka fo autorizasaun asesu ba dadus funsionáriu fó ba se, no se maki iha direitu ba assesu dados funsionario no oinsa halo monitorizasaun ?

Jelaskan prosedur pemberian akses ke data pegawai (siapa yang meminta, siapa yang menyetujui, langkah teknis), serta bagaimana akses tersebut dimonitor dan dicatat (mis. logging, audit trail, review berkala).

2 responses

R: Prosedimentu ka fó autorizasaun atu asesu ba dadus funsionáriu mak hanesan Parte HRD rasik no Finansas no Superior Másimu no Staff IT no mós individu no ba dadus hirak nee ida-idak asesu tuir nia prosedúr, hanesan tuir mai ne'e So parte HR, DE, DF ho Staff IT mak bele asesu ba dadus hotu no ba Staff IT so-bele asesu uain hira hetan autoriza husi HR no DE.

#### 4. Validation Link <https://forms.gle/16inr6TZaMzGZADH8>

https://docs.google.com/forms/d/1t6\_8ekoPJNZXF-afibPVMh8mBmvo5NRv5CKmtUGNT4/edit#responses

Untitled form

Questions Responses 1 Settings

Human Resources Division

1. Apakah Anda setuju bahwa akses tidak sah terhadap data pribadi pegawai dikategorikan sebagai risiko Tinggi?

Do you agree that Unauthorized Access to employee personal data should be classified as a High risk?

1 response

100%

● Setuju / Agree  
● Sebagian Setuju / Partially Agree  
● Tidak Setuju / Disagree

**TABLE A.1 INTERVIEW PROTOCOL**

|    |                                                                                                                                              |
|----|----------------------------------------------------------------------------------------------------------------------------------------------|
| No | General Information                                                                                                                          |
|    | Human resources division                                                                                                                     |
| 1. | Question                                                                                                                                     |
|    | Can you explain your role and responsibilities in managing employee data?                                                                    |
|    | Response                                                                                                                                     |
|    |                                                                                                                                              |
| 2. | Question                                                                                                                                     |
|    | What types of personal data are stored in the system?                                                                                        |
|    | Response                                                                                                                                     |
|    |                                                                                                                                              |
| 3. | Question                                                                                                                                     |
|    | How is employee data structured and stored in this institution? Is it stored in a data center, cloud, or locally (e.g., Excel or HR system)? |
|    | Response                                                                                                                                     |
|    |                                                                                                                                              |
|    | <b>Data Storage and Access</b>                                                                                                               |
| 4. | Question                                                                                                                                     |
|    | Where is employee data stored physically and digitally (local server, database, cloud, Excel files, etc.)?                                   |
|    | Response                                                                                                                                     |
|    |                                                                                                                                              |
| 5. | Question                                                                                                                                     |
|    | Who has the right to access the employee database (IT staff, HR, Finance, or supervisors)?                                                   |
|    | Response                                                                                                                                     |
|    |                                                                                                                                              |

|     |                                                                                                              |
|-----|--------------------------------------------------------------------------------------------------------------|
| 6.  | Question                                                                                                     |
|     | What is the procedure for granting access to employee data, and how is access monitored?                     |
|     | Response                                                                                                     |
|     |                                                                                                              |
| 7.  | Question                                                                                                     |
|     | Is there an activity log (audit trail) to record who accesses, modifies, or deletes personal data?           |
|     | Response                                                                                                     |
|     |                                                                                                              |
|     | Data Protection Mechanism                                                                                    |
| 8.  | Question                                                                                                     |
|     | How does the institution's system protect employee data during storage and transmission? Is encryption used? |
|     | Response                                                                                                     |
|     |                                                                                                              |
| 9.  | Question                                                                                                     |
|     | Are there firewall, IDS/IPS, or other network security systems protecting the database server?               |
|     | Response                                                                                                     |
|     |                                                                                                              |
| 10. | Question                                                                                                     |
|     | What is the password policy for accessing employee data? Are passwords changed periodically?                 |
|     | Response                                                                                                     |
|     |                                                                                                              |
| 11. | Question                                                                                                     |
|     | Is multi-factor authentication (MFA/2FA) implemented for accessing sensitive data?                           |
|     | Response                                                                                                     |
|     |                                                                                                              |

|     |                                                                                             |
|-----|---------------------------------------------------------------------------------------------|
| 12. | Question                                                                                    |
|     | Is there a backup system for employee data? How often is it performed and is it encrypted?  |
|     | Response                                                                                    |
|     |                                                                                             |
|     | <b>Policy and Training</b>                                                                  |
| 13. | Question                                                                                    |
|     | Are there written policies or regulations regarding employee data privacy and protection?   |
|     | Response                                                                                    |
|     |                                                                                             |
| 14. | Question                                                                                    |
|     | Have staff received training on personal data protection?                                   |
|     | Response                                                                                    |
|     |                                                                                             |
| 15. | Question                                                                                    |
|     | Is there a procedure to delete or deactivate accounts of resigned employees?                |
|     | Response                                                                                    |
|     |                                                                                             |
|     | <b>Insident History</b>                                                                     |
| 16. | Question                                                                                    |
|     | Have there been any incidents of data breaches, illegal access, or misuse of employee data? |
|     | Response                                                                                    |
|     |                                                                                             |
| 17. | Question                                                                                    |
|     | If such incidents occurred, how would they be handled?                                      |
|     | Response                                                                                    |
|     |                                                                                             |
| 18. | Question                                                                                    |

|     |                                                                                                   |
|-----|---------------------------------------------------------------------------------------------------|
|     | Did any incident result in legal, reputational, or financial consequences?                        |
|     | Response                                                                                          |
|     |                                                                                                   |
|     | <b>Risk Perception and Recommendations</b>                                                        |
|     | Question                                                                                          |
|     | In your opinion, what is the biggest risk to the confidentiality and security of employee data?   |
|     | Response                                                                                          |
|     |                                                                                                   |
| 19. | Question                                                                                          |
|     | In your opinion, what can be improved to strengthen employee data protection in this institution? |
|     | Response                                                                                          |
|     |                                                                                                   |
|     | <b>Unity Cyber Security Division</b>                                                              |
| 1.  | Question                                                                                          |
|     | Are there written policies or regulations regarding employee data privacy and protection?         |
|     | Response                                                                                          |
|     |                                                                                                   |
| 2.  | Question                                                                                          |
|     | Have staff received training on personal data protection?                                         |
|     | Response                                                                                          |
|     |                                                                                                   |
|     | <b>Data Center Division</b>                                                                       |
| 1.  | Question                                                                                          |
|     | Are there firewall, IDS/IPS, or other network security systems protecting the database server?    |
|     | Response                                                                                          |
|     |                                                                                                   |

|                                                   |                                                                                                              |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 2.                                                | Question                                                                                                     |
|                                                   | How does the institution system protect employee data during storage and transmission? Is encryption used?   |
|                                                   | Response                                                                                                     |
|                                                   |                                                                                                              |
| 3.                                                | Question                                                                                                     |
|                                                   | Is there a backup system for employee data? How often is it performed and is it encrypted?                   |
|                                                   | Response                                                                                                     |
|                                                   |                                                                                                              |
| <b>Information System Development Directorate</b> |                                                                                                              |
| 1.                                                | Question                                                                                                     |
|                                                   | How does the institution's system protect employee data during storage and transmission? Is encryption used? |
|                                                   | Response                                                                                                     |
|                                                   |                                                                                                              |
| 2.                                                | Question                                                                                                     |
|                                                   | What is the password policy for accessing employee data? Are passwords changed periodically?                 |
|                                                   | Response                                                                                                     |
|                                                   |                                                                                                              |
| 3.                                                | Question                                                                                                     |
|                                                   | Is multi-factor authentication (MFA/2FA) implemented for accessing sensitive data?                           |
|                                                   | Response                                                                                                     |

## APPENDIX B INTERVIEW RESULTS

The following section presents the results of the interviews conducted using the interview protocol provided in Appendix A.

### 1. Respondent Information I

Name : Abel Sarmento  
 Position : Chief of Human Resources  
 Agency : TIC TIMOR I.P  
 Length of service : 3.5 Years  
 Day, date : Tuesday, 2 September 2025

### 2. Respondent Information II

Name : Camilo Alves  
 Position : Staff Cyber Security  
 Agency : TIC TIMOR I.P  
 Length of service : 6 Years  
 Day, date : Tuesday, 2 September 2025

### 3. Respondent Information III

Name : Fidel Leite  
 Position : Staff Data Center  
 Agency : TIC TIMOR I.P  
 Length of service : 2 Years  
 Day, date : Tuesday, 4 September 2025

### 4. Respondent Information IV

Name : Jery Alves  
 Position : Staff Information System Development  
 Agency : TIC TIMOR I.P  
 Length of service : 3 Years  
 Day, date : Tuesday, 4 September 2025

**TABLE B.1 INTERVIEW RESULTS**

|    |                                                                                                                                                                                                                                                                                                          |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No | General Information                                                                                                                                                                                                                                                                                      |
|    | Human resources division                                                                                                                                                                                                                                                                                 |
| 1. | Question                                                                                                                                                                                                                                                                                                 |
|    | Can you explain your role and responsibilities in managing employee data?                                                                                                                                                                                                                                |
|    | Response                                                                                                                                                                                                                                                                                                 |
|    | As part of the Human Resources Division, my role and responsibilities in employee data management include ensuring the security, control, and proper storage of each employee's personal data. This includes maintaining employment contracts and personal identity documents.                           |
| 2. | Question                                                                                                                                                                                                                                                                                                 |
|    | What types of personal data are stored in the system?                                                                                                                                                                                                                                                    |
|    | Response                                                                                                                                                                                                                                                                                                 |
|    | The types of personal data stored include individual employment contracts, personal identity documents (such as Electoral Card and National ID), formal and non-formal education certificates, and individual bank account information.                                                                  |
| 3. | Question                                                                                                                                                                                                                                                                                                 |
|    | How is employee data structured and stored in this institution? Is it stored in a data center, cloud, or locally (e.g., Excel or HR system)?                                                                                                                                                             |
|    | Response                                                                                                                                                                                                                                                                                                 |
|    | Currently, employee data is stored within the HR Department locally in two formats: soft copy and hard copy. Since this data is considered confidential, access is limited to HR personnel and the respective individual employee. Some data has also been stored in the cloud and within the HR system. |
|    | <b>Data Storage and Access</b>                                                                                                                                                                                                                                                                           |
| 4. | Question                                                                                                                                                                                                                                                                                                 |

|    |                                                                                                                                                                                                                                                                                                                                                                    |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Where is employee data stored physically and digitally (local server, database, cloud, Excel files, etc.)?                                                                                                                                                                                                                                                         |
|    | Response                                                                                                                                                                                                                                                                                                                                                           |
|    | Employee data is stored both physically and digitally, including on local servers, databases, cloud storage, and Excel files.                                                                                                                                                                                                                                      |
| 5. | Question                                                                                                                                                                                                                                                                                                                                                           |
|    | Who has the right to access the employee database (IT staff, HR, Finance, or supervisors)?                                                                                                                                                                                                                                                                         |
|    | Response                                                                                                                                                                                                                                                                                                                                                           |
|    | Access rights to the employee database are granted to HR personnel, the Finance Division, top management/superiors, IT staff, and the respective individual employee.                                                                                                                                                                                              |
| 6. | Question                                                                                                                                                                                                                                                                                                                                                           |
|    | What is the procedure for granting access to employee data, and how is access monitored?                                                                                                                                                                                                                                                                           |
|    | Response                                                                                                                                                                                                                                                                                                                                                           |
|    | Access authorization is granted to HR, Finance, senior management, IT staff, and relevant individuals according to established procedures. Generally, only HR, Directorate Executives (DE), Finance Directorate (DF), and IT staff are allowed full access. IT staff may access the data only after receiving authorization from HR and the Directorate Executive. |
|    |                                                                                                                                                                                                                                                                                                                                                                    |
|    |                                                                                                                                                                                                                                                                                                                                                                    |
| 7. | Question                                                                                                                                                                                                                                                                                                                                                           |
|    | Is there an activity log (audit trail) to record who accesses, modifies, or deletes personal data?                                                                                                                                                                                                                                                                 |
|    | Response                                                                                                                                                                                                                                                                                                                                                           |
|    | Personal data is deleted only when an employee's contract has officially ended at TIC TIMOR I.P. HR informs the Finance Directorate and Data Center Directorate to deactivate the system                                                                                                                                                                           |

|     |                                                                                                                                                                                                                       |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | access and salary processing.                                                                                                                                                                                         |
|     | <b>Data Protection Mechanism</b>                                                                                                                                                                                      |
| 8.  | Question                                                                                                                                                                                                              |
|     | How does the institution's system protect employee data during storage and transmission? Is encryption used?                                                                                                          |
|     | Response                                                                                                                                                                                                              |
|     | The institution ensures confidentiality and integrity when storing or transmitting employee data by using official institutional email services and internally managed cloud systems maintained by the IT staff.      |
| 9.  | Question                                                                                                                                                                                                              |
|     | Are there firewall, IDS/IPS, or other network security systems protecting the database server?                                                                                                                        |
|     | Response                                                                                                                                                                                                              |
|     | Although this is outside my direct responsibility, to my knowledge the institution has implemented basic network firewall. However advanced protection namely cloudflare protection have not implemented.             |
| 10. | Question                                                                                                                                                                                                              |
|     | What is the password policy for accessing employee data? Are passwords changed periodically?                                                                                                                          |
|     | Response                                                                                                                                                                                                              |
|     | Human Resources collaborates with the Data Center and Information System Development Directorate to create user accounts and passwords. After receiving access, individuals may change their passwords independently. |
| 11. | Question                                                                                                                                                                                                              |
|     | Is multi-factor authentication (MFA/2FA) implemented for accessing                                                                                                                                                    |

|     |                                                                                                                                                                                                                                                |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | sensitive data?                                                                                                                                                                                                                                |
|     | Response                                                                                                                                                                                                                                       |
|     | Yes, multi-factor authentication is implemented for accessing sensitive data. Within the HR system, there are four authorized HR personnel, including the DCS Director. Only users with administrator privileges can access all employee data. |
| 12. | Question                                                                                                                                                                                                                                       |
|     | Is there a backup system for employee data? How often is it performed and is it encrypted?                                                                                                                                                     |
|     | Response                                                                                                                                                                                                                                       |
|     | Yes, employee data is backed up on TIC's internal servers. The Data Center team performs the backup process, while HR remains responsible for the data.                                                                                        |
|     | <b>Policy and Training</b>                                                                                                                                                                                                                     |
| 13. | Question                                                                                                                                                                                                                                       |
|     | Are there written policies or regulations regarding employee data privacy and protection?                                                                                                                                                      |
|     | Response                                                                                                                                                                                                                                       |
|     | Yes, data protection follows Decree Law No. 43/2016 of 14 October, concerning rules for access to official documents. Employees who improperly access or publish personal data may face sanctions under this decree.                           |
| 14. | Question                                                                                                                                                                                                                                       |
|     | Have staff received training on personal data protection?                                                                                                                                                                                      |
|     | Response                                                                                                                                                                                                                                       |
|     | Yes, relevant staff have received training and awareness programs on proper handling of personal data.                                                                                                                                         |
| 15. | Question                                                                                                                                                                                                                                       |

|     |                                                                                                                        |
|-----|------------------------------------------------------------------------------------------------------------------------|
|     | Is there a procedure to delete or deactivate accounts of resigned employees?                                           |
|     | Response                                                                                                               |
|     | Yes, there is an established procedure to delete or deactivate employee data when they resign or are no longer active. |
|     | <b>Insident History</b>                                                                                                |
| 16. | Question                                                                                                               |
|     | Have there been any incidents of data breaches, illegal access, or misuse of employee data?                            |
|     | Response                                                                                                               |
|     | No, there have been no such incidents to date, All incident were due to internet down.                                 |
| 17. | Question                                                                                                               |
|     | If such incidents occurred, how would they be handled?                                                                 |
|     | Response                                                                                                               |
|     | There have been no such cases so far.                                                                                  |
| 18. | Question                                                                                                               |
|     | Did any incident result in legal, reputational, or financial consequences?                                             |
|     | Response                                                                                                               |
|     | There have been no such cases to date.                                                                                 |
|     | <b>Risk Perception and Recommendations</b>                                                                             |
| 19. | Question                                                                                                               |
|     | In your opinion, what is the biggest risk to the confidentiality and security of employee data?                        |
|     | Response                                                                                                               |
|     | In my opinion, the greatest risk to confidentiality comes from                                                         |

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | individuals themselves, as employees may sometimes voluntarily share their own personal information with others.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 20. | Question                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|     | In your opinion, what can be improved to strengthen employee data protection in this institution?                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|     | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|     | Employees should increase awareness and be more cautious in protecting their personal information and confidentiality.                                                                                                                                                                                                                                                                                                                                                                                                              |
|     | <b>Unity Cyber Security Division</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 1.  | Question                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|     | Are there written policies or regulations regarding employee data privacy and protection?                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|     | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|     | <p>Yes, the institution applies internal regulations that have been formally established within the organization. Furthermore, TIC TIMOR I.P has adopted the international standard ISO/IEC 27001:2022.</p> <p>However, the implementation of this standard is not yet fully applied to all staff members. Currently, only the Cyber Division personnel have undergone formal testing and obtained certification related to ISO/IEC 27001:2022. Other divisions, including HR, are not yet fully certified under this standard.</p> |
| 2.  | Question                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|     | Have staff received training on personal data protection?                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|     | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|     | <p>Yes, staff members have received training related to the proper use and protection of personal data. However, the training is not conducted regularly or on a daily basis. It is usually provided during specific sessions or institutional programs rather than as a continuous routine activity.</p>                                                                                                                                                                                                                           |

|    |                                                                                                                                                                                                                                                                                                                                      |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                                                                                                                                                                                                                                                                                                                      |
|    | Data Center Division                                                                                                                                                                                                                                                                                                                 |
| 1. | Question                                                                                                                                                                                                                                                                                                                             |
|    | Are there firewall, IDS/IPS, or other network security systems protecting the database server?                                                                                                                                                                                                                                       |
|    | Response                                                                                                                                                                                                                                                                                                                             |
|    | Yes, the institution has implemented a firewall that is capable of functioning as an IDS/IPS (Intrusion Detection System / Intrusion Prevention System).                                                                                                                                                                             |
| 2. | Question                                                                                                                                                                                                                                                                                                                             |
|    | How does the institution's system protect employee data during storage and transmission? Is encryption used?                                                                                                                                                                                                                         |
|    | Response                                                                                                                                                                                                                                                                                                                             |
|    | Only data that is transmitted or sent digitally from the institution is encrypted to ensure data confidentiality and integrity.                                                                                                                                                                                                      |
| 3. | Question                                                                                                                                                                                                                                                                                                                             |
|    | Is there a backup system for employee data? How often is it performed and is it encrypted?                                                                                                                                                                                                                                           |
|    | Response                                                                                                                                                                                                                                                                                                                             |
|    | Yes, there is a backup system in place for employee data. The institution performs data backups whenever there are changes or updates to the employee information. By regularly performing backups and storing the data in the Data Center, the institution enhances data availability, integrity, and overall information security. |
|    | <b>Information System Development Directorate</b>                                                                                                                                                                                                                                                                                    |
| 1. | Question                                                                                                                                                                                                                                                                                                                             |
|    | How does the institution's system protect employee data during storage and transmission? Is encryption used?                                                                                                                                                                                                                         |
|    | Response                                                                                                                                                                                                                                                                                                                             |
|    | The institution implements several technical controls to protect employee data both during storage and transmission. Data stored within the system is secured through controlled access mechanisms                                                                                                                                   |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>and server-level security configurations managed by the Data Center and IT security team.</p> <p>For data transmission, official institutional communication channels, including secured email services and internally managed cloud infrastructure, are utilized. Encryption protocols are applied during data transmission to ensure confidentiality and integrity, particularly when data is transferred between systems or accessed remotely.</p> <p>These security measures are designed to align with information security best practices and to reduce the risk of data interception, unauthorized disclosure, or alteration.</p> |
| 2. | Question                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|    | What is the password policy for accessing employee data? Are passwords changed periodically?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|    | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|    | <p>The application system is developed collaboratively by the Human Resources (HR) Division and the Data Center (DC). Initially, a simple username and password are created and assigned to staff members. After receiving their login credentials, users are allowed to change their passwords independently. Once changed, the password becomes confidential and is fully the responsibility of the respective user. Password management thereafter depends on the individual user.</p>                                                                                                                                                   |
| 3. | Question                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|    | Is multi-factor authentication (MFA/2FA) implemented for accessing sensitive data?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|    | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|    | <p>No multi-factor authentication (MFA) has not implemented for assessing sensitive data. Currently system only rely on username and password.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### APPENDIX C MAPPING OF RISK ANALYSIS

| No | Threat Scenario                               | Related Question | Key Findings (Summary of Responses)                                                                                            | CIA Impact                    | Likelihood | Impact | Risk Score |
|----|-----------------------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------|------------|--------|------------|
| 1  | Unauthorized access to employee personal data | Q2, Q5, Q10, Q11 | Highly sensitive data (ID, bank accounts); multiple roles have access; weak password control; MFA not consistently implemented | C: High, I: Medium, A: Low    | 3          | 5      | 15         |
| 2  | Web exploitation leading to data extraction   | Q9               | Only basic firewall implemented; no advanced protection mechanisms                                                             | C: High, I: High, A: Medium   | 3          | 4      | 12         |
| 3  | DDoS attack causing HRMS unavailability       | Q16              | Previous incidents related to network or internet disruption                                                                   | C: Low, I: Low, A: High       | 4          | 3      | 12         |
| 4  | Insider privilege escalation                  | Q5, Q6           | Broad access rights; access control based on approval is not strictly enforced                                                 | C: High, I: High, A: Medium   | 3          | 4      | 12         |
| 5  | Ransomware infection affecting HR database    | Q14              | Security awareness training is not conducted regularly                                                                         | C: Medium, I: Medium, A: High | 3          | 4      | 12         |
| 6  | Backup failure or unsuccessful data recovery  | Q12              | Backup exists but no evidence of regular testing                                                                               | C: Low, I: Medium, A: Medium  | 3          | 3      | 9          |

|   |                                       |     |                                                                                |                              |   |   |   |
|---|---------------------------------------|-----|--------------------------------------------------------------------------------|------------------------------|---|---|---|
| 7 | Third-party vendor misuse             | Q5  | Data access involves multiple parties including IT and other related personnel | C: Medium, I: Medium, A: Low | 3 | 3 | 9 |
| 8 | Social engineering targeting HR staff | Q19 | Employees may unintentionally share personal information                       | C: High, I: Medium, A: Low   | 2 | 4 | 8 |

#### APPENDIX D DOCUMENTATIONS



## APPENDIX E EXECUTIVE SUMMARY

### Executive Summary

#### Purpose

This document presents the results of a security risk assessment conducted on the Human Resources Management System (HRMS) of the Human Resources Division at TIC TIMOR, IP. The assessment aims to identify potential risks affecting the security of employee personal data and provide practical recommendations to strengthen information security.

---

#### Methodology

The assessment was conducted using the OCTAVE Allegro methodology, a structured risk assessment framework that identifies critical information assets, analyzes potential threats and vulnerabilities, evaluates risk levels, and determines appropriate mitigation strategies.

---

#### Key Findings

The assessment identified several security concerns that may increase the organizations exposure to cyber threats, including:

- Absence of Web Application Firewall (WAF) protection.
- Weak access control mechanisms.
- Limited web security configuration.

These conditions may increase the likelihood of security incidents affecting employee personal data.

---

#### Risk Analysis

Based on the OCTAVE Allegro assessment, Unauthorized Access to Employee Personal Data was identified as the highest-priority risk with a High Risk rating. This risk is primarily associated with weaknesses in authentication and access control, which could lead to unauthorized disclosure of sensitive employee information.

Other identified threats, including web exploitation, DDoS attacks, insider privilege misuse, and ransomware, were assessed as Moderate Risk and should be addressed through appropriate security controls.

---

#### Recommendations

To reduce the identified risks, the following actions are recommended:

- Implement Multi-Factor Authentication (MFA).
  - Deploy a Web Application Firewall (WAF).
  - Strengthen password and access control policies.
  - Conduct periodic user access reviews.
  - Perform regular backup and recovery testing.
  - Improve system monitoring and vulnerability management.
  - Provide cybersecurity awareness training for HR personnel.
- 

#### Conclusion

The OCTAVE Allegro assessment provides a structured evaluation of the security risks affecting employee personal data within the HRMS. The findings indicate that improvements in authentication, access control, and preventive security measures are necessary to reduce organizational risk. Implementing the recommended controls will strengthen the confidentiality, integrity, and availability of employee personal data while enhancing the organization's overall cybersecurity posture.

## CURRICULUM VITAE

### Biography



Idalia Francisca Viegas was born in Dili, Timor-Leste, on January 15, 2004, as the beloved daughter of Justino Viegas Soares and Agueda Francisca Perreira. She is a Timorese citizen and a Catholic. She currently resides at Becora, Dili, Timor-Leste. She completed her elementary education from 2010 to 2015, then continued to junior high school from 2016 to 2018, and senior high school from 2019 to 2021, majoring in Natural Sciences (IPA) at Sta. Madalena de Canossa, where she graduated in 2021. In September 2022, she began her journey to pursue a bachelor's degree in Informatics Engineering at Universitas Pendidikan Ganesha in Bali - Indonesia. Throughout her studies, she developed a deep interest and passion. During her undergraduate studies, she developed a strong interest in cybersecurity, information security risk management, and information systems security.

As one of the requirements for obtaining the Bachelor of Computer Science degree, she completed a thesis entitled Risk Analysis of Employee Personal Data Security in the Human Resources Division of a Government Institution in Timor-Leste Using the OCTAVE Allegro Method. This research focuses on identifying, assessing, and prioritizing information security risks affecting employee personal data, as well as providing mitigation recommendations based on information security best practices. Through this study, she hopes to contribute to strengthening information security awareness and improving the protection of employee personal data within government institutions in Timor-Leste.