Securing Digi's **altHR** Applications Used In Operating Companies

August 2020

Version 03/2020

Notice

This document is provided for informational purposes only. It represents Digi's service "**altHR**" practices as of the date of issue of this document, which are subject to change without notice. Clients are responsible for making their own independent assessment of the information in this document and any use of Digi's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. The responsibilities and liabilities of Digi to its clients are controlled by Digi agreements, and this document is not part of, nor does it modify, any agreement between Digi and its customers.

Contents

Overview 4

Scope 4

Introduction to Digi's HR Application 5

Security Overview 6

Application Architecture 7

Data Encryption 8

User Authentication 8

Passwords 9

User Authorisation 9

Penetration Test 10

Vulnerability Assessment 10

Source Code Review 10

State-Of-The-Art-Hosting 11

Amazon EC2 11

Amazon S3 11

Disaster Recovery 11

Server Management Security 12

Data Ownership and Protection 13

Privacy by Design 13

- Principle 1: General Principle 13
- Principle 2: Notice and Choice Principle 14
- Principle 3: Disclosure 14
- Principle 4: Security Principle 14
- Principle 5: Retention Principle 14
- Principle 6: Access Principle 14
- Principle 7: Data Integrity Principle 14

Conclusion 15

References 16

Overview

HR softwares are becoming more relevant as companies grow in size. HR softwares help HR admins handle routine HR tasks and eliminate the need for paperwork associated with HR operations. Reducing time spent on these tasks helps companies improve overall efficiency and free up time for HR admins to work on higher impact work.

altHR is designed to provide features, functions and benefits for today's organisations. However, with such flexibility comes the need for a robust framework to address the creation, deployment and execution of secure and protected mobile and web applications, to reduce business exposure to associated risks.

This document will provide an overview of the **altHR** application, focusing in particular on the security and privacy aspects of the application. The purpose of this document is to help key decision makers understand the importance of secure applications before they can be deemed suitable to be used in organisations.

Scope

This document will discuss the importance of security and privacy for the application development and how **altHR** meets the industry benchmark for design, hosting and server security standards. Following the discussion on application security, this whitepaper will discuss the Privacy Policies built into **altHR** to protect the confidentiality of customer information.

This paper is not legal advice, and should not be relied on as legal advice. As each client's requirements will differ, Digi strongly encourages its clients to obtain appropriate advice on their implementation of privacy and data protection requirements, and more generally, applicable laws relevant to their business.

Introduction to Digi's HR Application

To help run organisations more efficiently, Digi has developed an HR application called '**altHR'**. There are multiple **altHR** modules within the app currently available for commercial use, specifically to help organisations efficiently manage onboarding, expense claims, travel authorisation, leave applications, case management, etc.

As the **altHR** application will become an increasingly integral HR management tool, it is important to assure employees that their personal data is protected and used only for legitimate business purposes. Having confidence in a highly secure environment, processes and policies built around **altHR**, customers will be more willing to adopt and use the full extent of application. Figure 1 summarises the customer journey of using the **altHR** application and the touchpoints that will be used as reference when discussing the security aspects of the application throughout this document. Considering the amount of sensitive and private data **altHR** is collecting, it is crucial to enforce security measures and stringent privacy policies to protect the confidentiality of data collected.

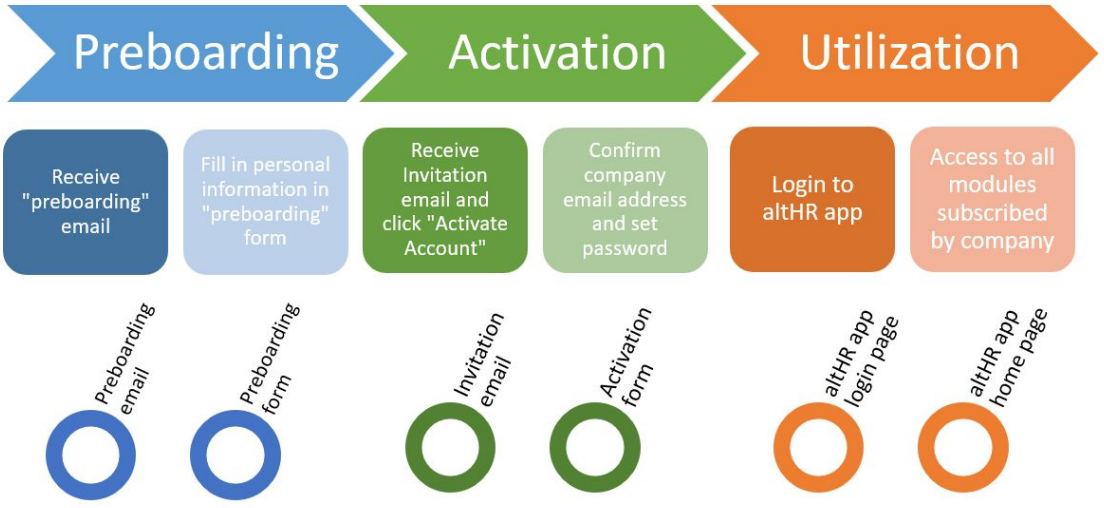

Figure 1: Customer journey layers of altHR application

Security Overview

End-to-end security is a vital aspect of Digi's mobile application development process, and these strict security considerations were applied throughout the development of **altHR**. It is common and prudent for organisations and employees to ask the following questions when considering adopting a new app into their environment:

- Where is my data being stored?
- How can I be sure that my data is secure?
- Who has access to my personal information?
- Is **altHR** compliant with laws and regulations?

altHR's storage of content and databases are fully hosted on Amazon Web Services (AWS). However, it is important to note that even though the AWS cloud solution is used for cloud computing and storage, **altHR** still maintains ownership and control of the application's content.

Based on Figure 2, **altHR**'s mobile application and web server communicate with the web application server and the database hosted by AWS. Hence, security of the content can be broken down into two areas using the "shared responsibility" model; security *in* the cloud and security *of* the cloud (Amazon Web Services, 2016). Digi ensures security in the cloud since they retain ownership and control over their data within the AWS environment. Even though data is not stored on-premise, **altHR** is fully responsible for ensuring the security in the cloud on the following:

- Customer data
- Identity and access management (IAM)
- Employee data encryption
- Server side encryption (File system and / or data)
- Network traffic protection (Encryption / Integrity / Identity)

altHR content is secured using relevant security tools and controls, which are further discussed in the *Secure by Design* and *Data Protection and Ownership* sections.

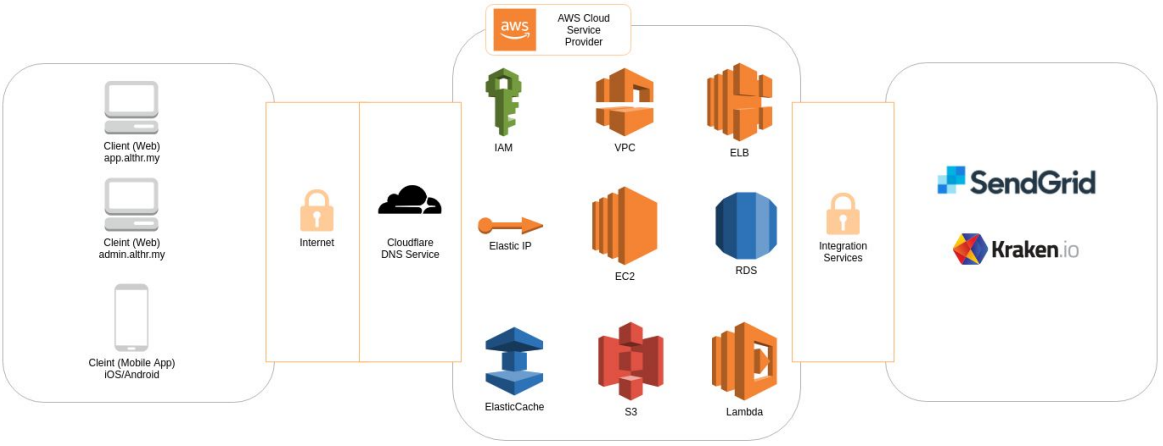

Figure 2: altHR application infrastructure diagram

AWS operates, manages and controls the components from the host operating system and virtualisation layer, and will be responsible for managing security of the underlying cloud environment.

For **altHR**, the AWS products used are;

1. AWS Identity and Access Management (IAM) to securely control users' access to AWS services.
2. Amazon Virtual Private Cloud (VPC) to provision a logically isolated section in the cloud where resources can be launched in a virtual network defined.
3. Amazon Elastic Cloud Computing (EC2) for hosting and scalable computing capacity.
4. Elastic Load Balancing to distribute incoming application traffic across multiple targets, such as Amazon EC2 instances. It features high availability, automatic scaling, and robust security.
5. Amazon Route 53 for extremely reliable Domain Name System (DNS) service.
6. Amazon S3 to store and retrieve any amount of media related data from anywhere. S3 provides comprehensive security and compliance capabilities that meet even the most stringent regulatory requirements.
7. Amazon Relational Database Service (RDS) to set up, operate, and scale a relational database in the cloud.

Further details on how AWS ensures security of the cloud can be found in the *State-Of-The-Art Hosting* section.

Secure by Design

Application Architecture

altHR is designed as a multi-layered application which is the recommended standard for mobile applications. The architecture partitions the applications' functionality into three independent layers: the presentation (mobile and browser client), business logic (application server) and data (database) layers.

It is common for the presentation layer not to have direct communication with the database layer. This implies that an employee will only need to interact with the presentation layer, with the Customer Journey Touchpoints being:

- Registration
- Login
- altHR Home Page
- Module based transactions depending on the module subscribed to by the employee's Company

Any communication performed is done via the business logic (basic validation checks) layer which executes its own security checks before allowing access to the data. This prevents requests from the mobile application to go directly to the database. An additional security measure includes the verification of the users' role at every request.

Data Encryption

As part of managing security in the cloud, **altHR** connects to the AWS environment through internet service providers. Current internet connections use secure protocols to encrypt communications to protect customer data and communications, including SSL Certification from Network Solutions, Secure Sockets Layer (SSL) or (Transport Layer Security). TLS is the standard security technology for creating an encrypted link between a web server and a browser (web application used by admin). The SSL link is created when the URL is green in colour, begins with “https://” and there is a padlock symbol either at the beginning or end of the URL.

User Authentication

If provided credentials match the database of authorised users’ information, employees are granted access to log into the application. Any incorrect password keyed in will disallow employees from logging into the application as shown in Figure 3.

However, if the wrong password is keyed in more than five consecutive times, employees will need to wait for 90 seconds before trying again. This security measure prevents hackers from accessing the application with unlimited tries.

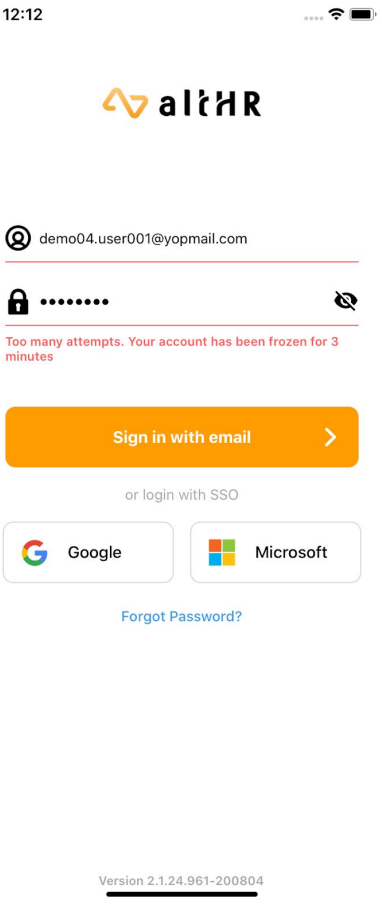

Figure 3: Invalid credentials when wrong password is keyed in

altHR has implemented Open Authorisation (OAuth) which is used for token-based authentication and authorisation on the Internet. With OAuth in place, employees' information can be used by the web application server without exposing the employees' password.

Passwords

During the login and / or registration process, employees are required to create their passwords to complete the account creation process. As **altHR** passwords are protected using sophisticated hashing and salting techniques, the application only stores hashes of passwords and never the passwords themselves.

To increase the security level of **altHR**, passwords must have the following combination:

- Special characters
- Capital letters
- Small letters
- Numeric
- Minimum of 8 characters

Companies can opt for a change of passwords at a set frequency to combat identity theft and prevent unauthorised individuals from gaining access into employees' personal and professional accounts.

User Authorisation

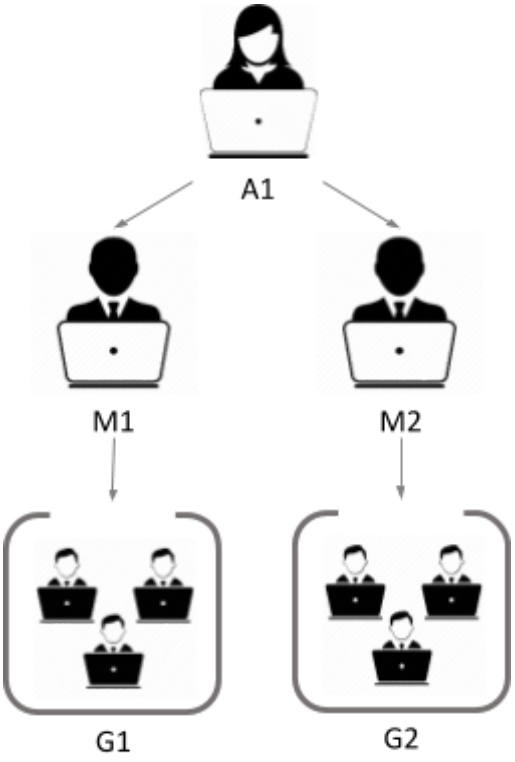

Figure 4: Diagram of user management roles giving them permission to selected data

In **altHR**, employees can fill in forms on the app before submitting it to their managers for approval. It is important to note that employees will not be able to view other employees' data and similarly, managers are only allowed to view and approve submissions for certain groups of employees. Ultimately, the admin will have the complete overview of data as they will need to manage employee data.

User authorisation is controlled via dynamic roles-based security. Roles will be allocated to employees such as HR admin, line manager or employee. **altHR** will then perform dynamic permissions allocation to the individual employee to view, approve, edit or delete information, or access different areas of functionality, based on their designation in the company.

Penetration Test

In addition to AWS's security measures to block unauthorised access to their infrastructure, Digi employs specialist certified vendors to subject altHR to frequent quarterly penetration testing. This step is crucial to test against security vulnerabilities and is done by attempting to gain resources without knowledge of emails and passwords.

Using an untested mobile application which may contain security bugs makes clients' data vulnerable and the goal of this test is to help increase security of the computing resources. With penetration tests applied frequently to **altHR**, employees are assured a worry-free experience on the app since it is tested for secure data storage, authentication and authorisation and proper session handling.

Vulnerability Assessment

altHR has gone through vulnerability assessments performed by Digi's in-house security team and / or Digi's appointed vendors. The assessment's purpose is to define, identify and classify security holes (vulnerabilities) in **altHR**, the network and communications infrastructure. It can also predict the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

Like the penetration test, quarterly vulnerability assessments are carried out to ensure all employee information stored in **altHR** are well protected.

Source Code Review

Source code review has been quoted many times as the single-most effective technique for identifying security flaws. When used with automated tools and manual penetration testing, code review can significantly increase cost effectiveness of **altHR**'s security verification effort.

Source code review provides Digi an internal view of **altHR**'s code quality and potential security issues relating to its design. By reviewing how altHR is developed internally before deployment, Digi can detect and fix software vulnerabilities before they can be exploited for malicious purposes.

State-Of-The-Art Hosting

AWS is one of the world's leading cloud infrastructure service providers, whose data centres are proven, secure, reliable and certified with ISO 27001, SOC 1/SSAE 16, SOC 2, SOC 3 and more. AWS's 27018 certification ensures that the system of controls that are in place specifically addresses and protects the privacy of **altHR**'s employee data.

Amazon EC2

Amazon EC2 is used to provide resizable computing capacity using server instances in AWS' data centres. Security within Amazon EC2 is provided on multiple levels: the operating system (OS) of the host platform, the virtual instance OS or guest OS, a firewall, and signed API calls. The goal is to prevent data contained within Amazon EC2 from being intercepted by unauthorised systems or users and to provide Amazon EC2 instances themselves that are as secure as possible without sacrificing the flexibility in configuration that customers demand (Amazon Web Services, 2016).

Amazon S3

Amazon Simple Storage Service (S3) allows you to upload and retrieve data on the web anytime, anywhere. Access to data stored in Amazon S3 is restricted by default and only AWS account owners have access to Amazon S3 resources they create. Amazon S3 supports user authentication to control access to data. The following access control mechanisms are used in this respect:

- **Identity and Access Management (IAM) Policies**
  Enables the **altHR** account owner to create and manage multiple users under a single AWS account
- **Access Control Lists (ACLs)**
  To give read or write employee data access to groups of users
- **Bucket Policies**
  Enabling centralised management of permissions, the **altHR** account owner can add or deny permissions across employee data

Data can be securely uploaded or downloaded to Amazon S3 via SSL endpoints using the HTTPS protocol. Additional security includes using the Server Side Encryption (SSE) option or the Server Side Encryption with Customer-Provide Keys (SSE-C) option to encrypt data stored-at-rest. Amazon S3 provides the encryption technology for both SSE and SSE-C (Amazon Web Services, n.d.).

Disaster Recovery

In the event of a disaster, **altHR** owners can either contact altHR support or launch AWS resources to ensure business continuity. **altHR** support currently performs disaster recovery on the application failure side. What constitutes an application failure in **altHR**'s core system should be discussed and defined upfront between **altHR** and the **altHR** owner, in terms of unacceptable results for the business, users or customers. Failures or threats that have been defined will be assessed and assigned with Recovery Point Objective (RPO), Recovery Time Objective (RTO), mitigation and recovery steps. Our business continuity and disaster recovery plan will be documented in detail and vetted through an exercise after implementation.

For basic disaster recovery, **altHR** clients will submit a ticket to **support@altHR** via the ticketing system with required information. Based on the severity of the ticket, it will be resolved within the given Service-Level Agreement (SLA).

In case of a disaster, the emergency call list will need to be used. The support team will be contacted and assembled to:

- Establish facilities with an emergency level of service within 2 business hours
- Restore key services within 4 business hours of the incident
- Recover to business-as-usual state of affairs within 8 to 24 hours of the incident

Besides that, AWS S3 can also be used as it is a highly durable storage infrastructure designed for mission critical and primary data storage. Data is redundantly stored on multiple devices across multiple facilities within a region, designed to provide a durability of 99.999999999% (11 9s). AWS provides further protection for data retention and archiving through versioning in Amazon S3, AWS, AWS MFA, bucket policies and AWS (IAM). Hence, it is an ideal destination for backup data that might be needed quickly to perform a restore. Transferring data to and from Amazon S3 is typically done through the network, and is therefore accessible from any location.

Of course, the backup of your data is only half of the story. If disaster strikes, you'll need to recover your data quickly and reliably. Amazon EC2 provides resizable compute capacity in the cloud. Within minutes, new Amazon EC2 instances can be created, which are virtual machines and fully controlled by **altHR**. Therefore, the backup data stored in AWS S3 can be used to restore a system to a new Amazon EC2 instance easily.

Server Management Security

altHR data is not stored on-premise and **altHR** owners will not have physical access to the AWS data centre or physical machines, as this is prohibited by Amazon. However, AWS has world-class, highly secure data centres utilising state-of-the-art electronic surveillance and multi-factor access control systems. Data centres are staffed 24x7 by trained security guards, and access is authorised strictly on a least privileged basis.

altHR owners will have access to virtual machine instances for maintenance purposes, applying security updates, monitoring and ensuring backups are occurring successfully. This access is only provided to designated IT security teams.

Data Protection and Ownership

Considering the amount of sensitive information being collected by **altHR**, Digi is careful to maintain strong internal procedures in relation to the handling and safeguarding of employee and customer data to protect these individuals' privacy.

Privacy by Design

altHR is designed with a privacy-first approach, promoting data protection compliance throughout the entire engineering process. It was built to comply with the Personal Data Protection Act 2010 (PDPA) which comprises seven data protection principles forming the basis of protection. **altHR** is compliant to industry standards for collecting, managing, dealing with, using, disclosing and handling personal data.

Principle 1: General Principle

Personal data is only processed once the employee has given his or her consent.

Consideration:

- Employees are informed or consent sought by their Company before their personal data is entered into **altHR**
- **altHR** only collects adequate data (not excessive) in relation to the services offered
- Notification about the purpose for which employees' information is collected, used or disclosed is provided in Digi's Privacy Notice (refer to Figure 5)

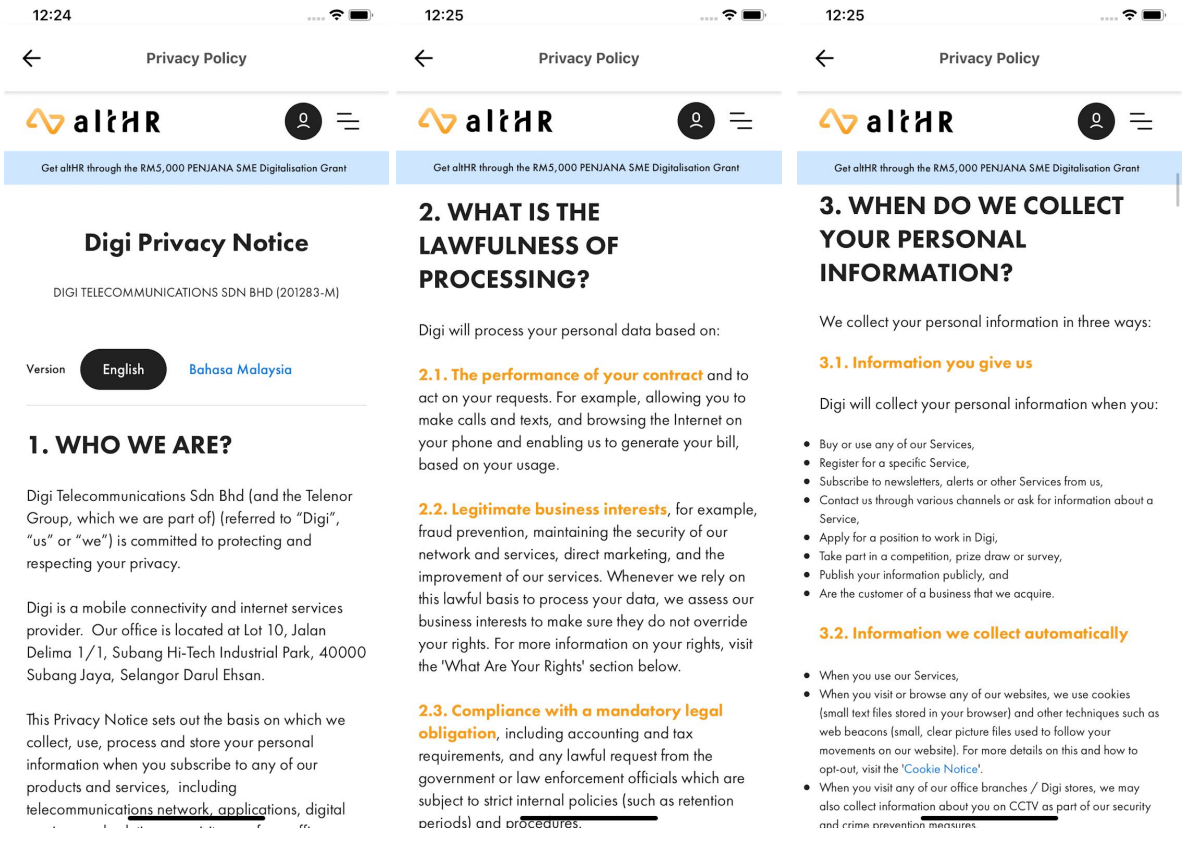

Figure 5: Digi Privacy Notice

Principle 2: Notice and Choice Principle

altHR informs the employee's Company the purposes for which their personal data is being collected and processed.

Consideration:

- Notification about the purpose for which employees' information is collected, used or disclosed is provided in Digi's and **altHR** Privacy Notice

Principle 3: Disclosure

Personal data is only disclosed with consent, and only for the purposes disclosed to the employee.

Consideration:

- Notification about the purpose for which employee's information is collected, used or disclosed is provided in **altHR**'s Privacy Notice

Principle 4: Security Principle

altHR takes practical steps to protect personal data from loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Consideration:

- Host of information security controls including (full details can be found in the *Secure by Design* section):
- Password Policy
- Audit Logs
- Encryption via HTTPS (SSL certified)

Principle 5: Retention Principle

Personal data is not kept longer than the end of efficiency (EOE) plus seven years for the fulfilment of the purpose for which the personal data was collected.

Consideration:

- In-built governance on retention period

Principle 6: Access Principle

Digi provides employee access to their personal data and ability to correct their personal data.

Consideration:

- **altHR** provides employees the access and option to update data

Principle 7: Data Integrity Principle

Digi takes all reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up-to-date, having regard to the purpose for which the personal data was collected.

Consideration:

- **altHR** provides employees the access and option to update data

Conclusion

altHR is a powerful mobile application created to manage HR services of a company and is designed to be secure in the cloud. Digi has carefully mapped out the customer's (employee's) journey when using **altHR** and has ensured that each step of the application is secure from various security aspects. Together with AWS hosting which guarantees security of the cloud, it is an application well worth of an investment for a seamless experience for employees, managers and administrators.

Digi employs core security-oriented design and coding principles that put the platform through a series of checks and balances to ensure data collected by **altHR** is secure and private as discussed in this document. Scheduled and ad hoc audit and compliance are frequently carried out to detect problems early and keep information security in place. As a mobile application provider, Digi has applied the strictest measures in protecting customer data as outlined by this document.

References

Amazon Web Services. (2016). Overview of Security Processes.

Amazon Web Services. (2016). Using AWS in the Context of Malaysian Privacy Considerations.

Common Terminology

altHR – Digi who owns **altHR**