Information Security
Company Policies
A Handbook

HR Easily Pte Ltd
June 2021

Revision History

Date	Version	Description	Author	Approver	Date Approved
1 Dec 2020	1.00	Implementation of new Information Security Policies	Security Team	Management	1 Dec 2020
5 Mar 2021	2.00	- Breach notification policy to reflect amendments of PDPA 2021 - Personal data protection policy	Security Team	Management	5 Mar 2021
10 Mar 2021	2.00	Updated footer version	Security Team	-	-
25 June 2021	3.00	Removed Data Retention from Backup Policy	Security Team	Management	25 June 2021
25 June 2021	3.00	Added Section 17: Data Retention, Archiving and Destruction Policy	Security Team	Management	25 June 2021

Table of Contents

InfoSec Handbook

Overview

1. Introduction

This document defines the organisation's Information Security Framework.

HRe's InfoSec framework contains a list of documents and policies that defines the HRe's cybersecurity program. These documents are the cornerstone of the information security framework that reflects HRe's security perspective and the management's strategy for securing data and information.

1.1. Commitment

The HRe management and security team commit to the continual improvement of the information security of the organisation.

1.2. Scope

All employees, contractors, consultants, temporary and other workers at HReasily and its subsidiaries must adhere to this policy.

This policy applies to any equipment and information systems that are owned, operated, or leased by HReasily or registered under a HReasily-owned internal network domain.

This policy also applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Personally Identifiable Information (PII) or Protected Health Information (PHI) of HRe members.

Bring-Your-Own-Device Policy: This policy applies to all HRe employees, including full and part-time staff, contractors, freelancers, and other agents who use a personally-owned device to access, store, back up, or relocate any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust HRe has built with its clients, partners, and other interested parties.

Consequently, employment at HRe does not automatically guarantee the initial or ongoing ability to use these devices to gain access to organizational networks and information.

1.3. Compliance Measurement

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

1.4. Exceptions

Any exceptions to the policy must be approved by the Security Team and documented.

1.5. Non-Compliance

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

2. Definition of Terms

2.1. Expressions

The following definitions apply in understanding how to implement and interpret these policies according to RFC 2119 and ISO foreword

- "must" indicates a requirement
- "should" indicates a recommendation
- "may" is used to indicate that something is permitted
- "can" is used to indicate that something is possible, for example, that an organization or individual is able to do something

2.2. Terms

Anonymised data

Anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the natural person is not or no longer identifiable. The principles of data protection should therefore not apply to such anonymous information, including for statistical or research purposes.

Critical asset

Assets that impact confidentiality, integrity, and/or availability and support business mission and functions. Critical assets can include patents and copyrights, corporate financial data, customer sales information, human resource information, proprietary software, schematics, and internal processes.

Configuration compliance

The process (manual or automated) to ensure configuration control. This includes proactively monitoring and protecting the IT infrastructure that affects a business' viability (e.g. compliances necessary for obtaining or renewing a business license) as well as compliance and security initiatives.

Exception Policy

Technical limitation or infeasibility, and business requirements may justify exceptions to such compliance policies. Such exceptions must be documented and approved according to the relevant policies.

Password rotation

Changing of passwords on a regular basis. The passwords should follow the determined password policies set by the organisation. This is a control in place for shared accounts especially service accounts where MFA cannot be practically implemented.

Personal data

From PDPA: "Personal data" is defined to mean data, whether true or not, about an individual who can be identified from that data.

From GDPR: 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Table 1: *Special Categories of Personal Identifiable Information (PII)*

Special categories of PII	Description
Genetic personal data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
Biometric personal data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic(fingerprint) data;
Sensitive personal data	Personal data that, by their nature, is particularly sensitive in relation to fundamental rights and freedoms and these merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. These sensitive personal data include personal data revealing racial/ethnic origin, sex life, and sexual orientation. Note that use of the term, racial origin in this policy does not imply an acceptance by the organisation of theories which attempt to determine the existence of separate human races.
Data concerning health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Pseudonymisation

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a

natural person by the use of additional information should be considered to be information on an identifiable natural person

Sensitive data

Sensitive data is a generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this policy. This term is often used interchangeably with confidential data.

Server

A server is a host that provides one or more services for other hosts over a network as a primary function. For the purposes of this document, a host that does not provide services for other hosts as a primary function, but incidentally provides one or a few services for maintenance or accessibility purposes, is not considered a server.

Server configuration guide

A set of baseline configurations set by the Infra/Security team to ensure compliance to security best practices and documented controls. This could be in a form of code, document or a run-book.

Whitelisting

The practice of explicitly allowing authenticated and authorised entities access to a particular resource, service, access or application.

Should there be a need to implement only one approach, the whitelisting approach is preferred where it is practical. Ex. Input Validation by OWASP

3. Roles and Responsibilities in Security Management

3.1. Information Officer

The Information Officer provides advisory services for the protection of information systems for the entire organization. The Information Officer is responsible for the following activities:

- Coordinating the development and maintenance of the organization's information security policies, standards, and procedures
- Coordinating the development and maintenance of the organization's change control and management procedures
- Ensuring the establishment of, and compliance with, consistent IT security policies for departments throughout the organization.

Note: As of this writing, the Chief People Officer takes on the role of the Information Officer.

3.2. Information Security Officer (ISO)

The ISO is responsible to oversee the implementation of and compliance with the standards, rules, and regulations specified in the organization's security policy.

- Ensuring that security procedures are developed and implemented
- Ensuring that security policies, standards, and requirements are followed
- Ensuring that all critical systems are identified and that contingency planning, disaster recovery plans, and continuity of operations plans exist for these critical systems
- Ensuring that critical systems are identified and scheduled for periodic security testing according to the security policy requirements of each respective system.

Note: As of this writing, the Chief Technology Officer takes on the role of the ISO.

3.3. Information Systems Security Officers

Information Systems Security Officers (ISSO) are responsible for overseeing all aspects of information security within a specific organisational entity. They ensure that the organization's information security practices comply with organisational and departmental policies, standards, and procedures. ISSOs are responsible for the following activities associated with servers:

- Developing internal security standards and procedures for the servers and supporting network infrastructure
- Cooperating in the development and implementation of security tools, mechanisms, and mitigation techniques

- Maintaining standard configuration profiles for the servers and supporting network infrastructure controlled by the organization, including, but not limited to, OSs, firewalls, routers, and server applications
- Maintaining operational integrity of systems by conducting security tests and ensuring that designated IT professionals are conducting scheduled testing on critical systems.

3.4. Server, Network, and Security Administrators

Server administrators are system architects responsible for the overall design, implementation, and maintenance of a server. Network administrators are responsible for the overall design, implementation, and maintenance of a network. Security administrators are dedicated to performing information security functions for servers and other hosts, as well as networks.

Organizations that have a dedicated information security team usually have security administrators. On a daily basis, server, network, and security administrators contend with the security requirements of the specific systems for which they are responsible.

Security issues and solutions can originate from either outside (e.g., security patches and fixes from the manufacturer or computer security incident response teams) or within the organization (e.g., the security office). The administrators are responsible for the following activities associated with servers:

- Installing and configuring systems in compliance with the organizational security policies and standard system and network configurations
- Maintaining systems in a secure manner, including frequent backups and timely application of patches
- Monitoring system integrity, protection levels, and security-related events
- Following up on detected security anomalies associated with their information system resources
- Conducting security tests as required.

4. Information Security

4.1. What is information security?

Information security (or infosec) is the safeguarding of our company's information asset according to the benchmark model: C-I-A approach:

4.1.1. Confidentiality

Access to company information is restricted to authorized personnel. Unauthorized access to information must not be permitted. For example, human resources are granted privileged access to staff leave records.

4.1.2. Integrity

Ensures that information is accurate and free from errors. Guards against unauthorized and improper modifications, destruction and tampering of data. For example, database integrity checks.

4.1.3. Availability

Ensures timely and reliable access to company information assets at all times. For example, the prevention of Denial of Service (DOS) attacks

4.2. Responsible Disclosure

If you believe there is a security breach and/or privacy violation that impacts the confidentiality, integrity and availability of company information, you must report this immediately to: security@hreasily.com

Similarly, anyone can report such violations through our responsible disclosure page: https://hreasily.com/responsible-disclosure/

We accept responsible disclosure reports done in good faith with the following information:

- Description of vulnerability (if applicable)
- Proof of concept or replication steps
- Trace dump or HTTP request (optional)

5. Guidelines and Processes

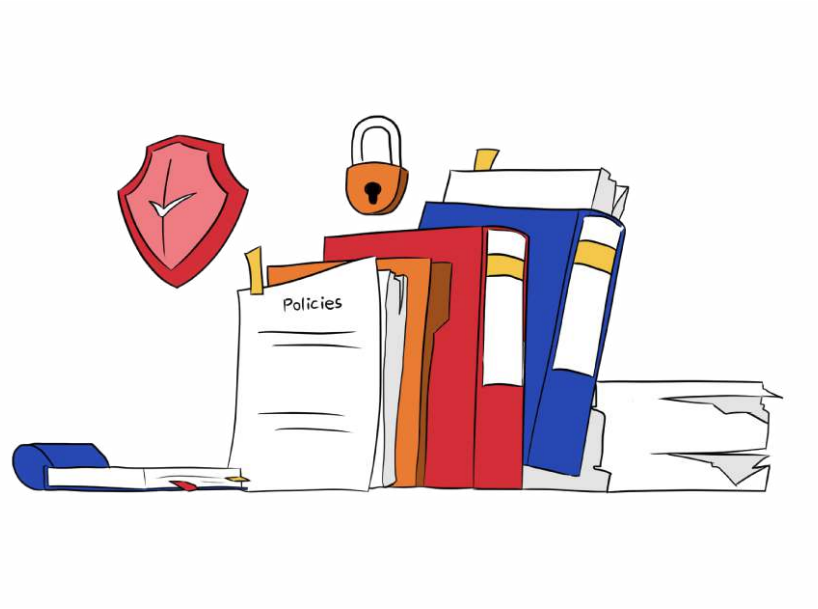
The following are the relevant guidelines, procedures and processes mentioned throughout this document. More will be added as the need arises.

- **Change Management and Review Process**
  - Change Management
  - Review Procedure
  - Vendor Assessment
- **Information Sharing - Traffic Light Protocol**
- **Server Baseline Guidelines**
- **Password Construction Guidelines**
- **Cryptographic Standards Guidelines**
- **Telework and Small Office Network Security Guidelines**
  - Home Network Security Checklist
- **Mobile Security Guidelines**
- **Incident Response - Vulnerability Management**
  - Vulnerability Rating Taxonomy
  - Severity Rating Scale and Table

Note: These guidelines are available in our Security space in Confluence. Check the Security space for updates.

InfoSec Handbook

Policies



6. Information Classification and Handling Policy

6.1. Purpose

This policy ensures that information is protected at an appropriate level by setting clear directions on how to create, use and control information based on the level of sensitivity, criticality and value to HRe as required within the organization's Cyber Security Framework.

6.2. Classification of data

Information classification, in the context of this policy is the classification of data based on the level of sensitivity and impact to our company should the data be disclosed, altered, or destroyed without authorisation.

The classification of data is the first step in determining baseline security controls appropriate for safeguarding data or assets controlled or owned by HRe.

6.2.1. Classification criteria

- value of information - based on the impacts assessed during risk assessment
- criticality of information
- sensitivity of information
- compliance with regulations

6.2.2. Color coding schemes

Confidentiality levels use the TLP scheme: RED AMBER GREEN WHITE. See Information Sharing - Traffic Light Protocol for more information.

6.3.

6.4. Confidentiality level

All information must be classified into one of the four (4) sensitivity or confidentiality levels.

Table 2: *Table of Confidentiality levels*

Confidentiality Level	Business Impact	Description
CONFIDENTIAL	**HIGH**	**Classification Criteria:** Unauthorized disclosure, alteration or destruction of that data would result in significant level of risk to HRe and its affiliates. Unauthorised disclosure or modification of data or resources could result in significant fines or penalties, regulatory action or civil, administrative or criminal violations. There are also inherent significant risks to the company's reputation and business continuity along with harm or impairment to employees, users and partners. **Examples:** • Documents containing proprietary information such as source codes, mock-ups, design documents, process and architecture designs, technical specifications, quality assurance test scripts and results; • Results of security tests (penetration testing reports), documents needed to comply with third-party assessments or audits; • PII, financial account numbers, credit or debit card numbers and financial account security codes, access codes, or passwords; • User credentials such as a username or email address, in combination with a password or security question and answer that would permit access to an online account; • Passwords, PINs and passphrases, or other authentication secrets that can be used to access or manage IT resources; • Access and refresh tokens **Access Restriction:** Information is never shared publicly. **CONFIDENTIAL** data has the most limited access and requires the highest level of protection and security. Sharing information with third-party affiliates requires: • signed Non-Disclosure Agreement (NDA) and • the approval from C-level e.g. Chief Technology Officer (CTO) • if it impacts privacy, approval needed from the Data Protection Officer (DPO) Note: "For my eyes only"
RESTRICTED	**MODERATE**	**Classification Criteria:** Data that is usually ***compartmental*** or ***departmental*** that might not pose a significant level of risk but must be kept restricted for other reasons or on a need-to-know basis. **Examples:** • Redacted documents such as mock-ups, design documents and process documents that do not contain information; • Reports such as Penetration Testing results, QA reports, and Incident reports with redacted information; • Security camera recordings, building entry records; • Infrastructure data: building plans, control systems, utilities, networks; • IT security information, exception requests and system security plans; • Audit Logs (access logs, application logs); • Personnel records not containing any confidential information;

		• Pseudonymised personal information; • Issue and vulnerability tracking system; • File servers supporting business operations **Access Restrictions:** Information is never shared publicly. **RESTRICTED** data has moderately limited access and requires a higher level of protection and security. Sharing information with third-party affiliates requires: • signed Non-Disclosure Agreement (NDA) and • the approval from C-level e.g. Chief Technology Officer (CTO) • if it impacts privacy, approval needed from the Data Protection Officer (DPO) Note: "I can *probably* share this with the rest of my team members."
INTERNAL-USE	**LOW**	**Classification Criteria:** Data may not be explicitly protected by statutes or other contractual regulations, but are not commonly intended for public use or access and should only be accessed on a need-to-know basis. Unauthorized disclosure or modification of P2 data could result in minor damage or small financial loss, or cause a minor impact on the privacy of an individual or group. All data and information that is not explicitly classified should be treated as **INTERNAL-USE** data. **Examples:** • Redacted documents such as policies, guidelines and procedures that do not contain or information; • Redacted incident reports that do not contain or information; • Compliance and certification reports (e.g. ISO 27001, SOC 2 Type II reports); • Informational knowledge base; • Licensed software keys and subscription electronic resources; • Internal-use API: https://api.hreasily-uat.com/v2; • Non-public research using publicly available data for marketing; **Access Restrictions:** Information is never shared publicly. **INTERNAL-USE** data has the lowest access and requires low levels of protection and security. Sharing information with third-party affiliates requires: • the approval from C-level e.g. Chief Technology Officer (CTO) • if it impacts privacy, approval needed from the Data Protection Officer (DPO) Note: "I can share this with the rest of the company."
PUBLIC	**MINIMAL**	**Classification Criteria:** Unauthorized disclosure, alteration or destruction of that data would result in little or no risk to HRe and its affiliates. **Examples:** • Press releases; • Security advisories; • Publicly-released incident reports; • Public-facing informational websites; • Public event calendars; • Hours of operation; • Parking regulations;

		• Published research, white papers and case studies; • Public knowledge databases; **Access Restrictions:** Information is available or can be shared to the public. While little or no controls are required to protect the confidentiality of **PUBLIC** data, some level of control is required to prevent unauthorized modification or destruction of **PUBLIC** data. Note: "I can share this with the world!"

6.5. Information Sharing

Granting access of **RESTRICTED** and **CONFIDENTIAL** documents to any **internal staff** does not need approval from the C-level. However, be mindful of the access restrictions specified from the Table of Confidentiality Levels.

For example, we currently have two (2) incident reports created: one full incident report with **RESTRICTED** classification (technical details, business impact, etc), and another with **INTERNAL-USE** classification. Both of these documents MUST NOT be shared to customers (external parties or the public) without an existing signed NDA form and approved by C-level officers.

When the **INTERNAL-USE** document is rewritten into a revised (easily digestible form) or redacted form (removal of sensitive information) for external parties, the resulting document retains its classification. That is, the incident report IS NOT considered a PUBLIC use document because data is shared across other parties on a need-to-know basis.

- Tech team → create → Full incident report → RESTRICTED use
- Tech team → create → Incident report for customer → Support → INTERNAL-USE → Rewrite → INTERNAL-USE → NDA/Approval → Share to Third party

7. Access Control Policy

The following access control procedures are implemented for onboarding starters (when a staff newly joins or moves from one role to another or from one department to another), or for off-boarding employees (leavers).

7.1. New Hires and Transfers

7.1.1. *Approval*: HR provides the go-ahead that appropriate checks are completed against new hires (e.g. background checks, sign-off of employment contract and acknowledgement of policies) before an access request is made

7.1.2. *Logical access (IT/HR)*: Once approval has been secured, the request is acted on. That is, issue of laptop, licenses, setup of HReasily account, Google (email, Gdrive) and the official chat communication tool (i.e. Discord).

7.1.3. *Data Access Request (HR)*: Appropriate access request is sent to line or department managers. For example, access to source code control, Jira, Confluence, or VPN.

7.1.4. *Sensitive Data Access (Head of Departments)*: Access of sensitive data is granted according to the Principle of Least Privilege by explicit approval by each head of department . For example, access to any production servers or database access.

7.1.5. *Physical Access (IT/HR)*: Access card (door pass) is issued, the serial number is logged and maintained by IT/HR. This is applicable for which HRe maintains an office such as Singapore, Thailand and Malaysia.

7.2. Leavers

7.2.1. *Notification (HR)*: Once the resignation letter is accepted - IT or HR operations proceeds to immediately deactivate the company accounts and prevent access to the network.

7.2.2. For cases of exceptions when the account has to remain active for a reasonable time, passwords are rotated until the account has been completely deactivated or removed.

7.2.3. *Timeline (IT/HR)*: Revocation of access must be completed on the same day as the last day or the termination day.

7.2.4. *Return of organisation-owned laptop (IT/HR)*: Laptops must be returned to the company on the last day. Line managers must ensure that the laptops had been safely returned to the company.

7.2.5. Return of access card (IT/HR): Access card (door pass) must be surrendered to the company on the last day. This should be logged by IT/HR and deactivated.

7.2.6. Audit (IT/HR/Security team): IT team ensures returned laptops are checked and securely wiped. The IT/HR together with the security team conduct audit for the list of accesses on company accounts to ensure all leavers have their accesses revoked.

7.3. General

The following access control should be followed by everyone who is part of the HRe organisation:

7.3.1. Only authorized users are granted access to information systems, and users are limited to defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual to provide individual accountability and attribution.

7.3.2. Any User (remote or internal), accessing networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- Biometric identification
- Password
- Personal identification number
- Token

7.3.3. All workstations used for this business activity, no matter where they are located, must use an access control system approved by the company.

7.3.4. Active workstations are not to be left unattended for prolonged periods of time. Refer to the Acceptable Use Policy to minimize the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

7.3.5. Disclosure Notice: A notice warning that those should only access the system (e.g. servers) with proper authority will be displayed initially before signing on to the

system. The warning message will make clear that the system is a private network or application and unauthorized users should disconnect or log off immediately.

7.3.6. System Access Controls: Access controls will be applied to all digital information based on the company's Data Classification Policy to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

7.3.7. Access Approval: System access will not be granted to any user without appropriate approval.

7.3.8. The relevant department (e.g. HR, IT) must immediately notify the System/Security Administrator and report all significant changes in end-user duties or employment status.

7.3.9. User access MUST BE immediately revoked if the individual has been terminated.

7.3.10. User privileges are to be appropriately changed if the user is transferred to a different role.

7.3.11. Least Privilege: Users will be granted access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required in performing their jobs.

7.3.12. Confidential and Critical Systems: Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access
- All privileged commands must be traceable to specific user accounts

7.3.13. Logs: In addition, logs of all inbound access into the company's internal network by systems outside of the defined network perimeter must be maintained.

7.3.14. Audit trails for confidential systems should be backed up and stored in accordance with Back-up and Disaster Recovery Plan.

7.3.15. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons.

7.3.16. All logs must be audited on a periodic basis.

7.3.17. Audit results should be included in periodic management reports.

7.3.18. Unauthorized Access: Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems.

7.4. Access for Non-Employees

7.4.1. Individuals who are not employees, contractors, consultants, or business partners MUST NOT be granted privileges to access the information systems.

7.4.2. Before any third party or external partner is given access to the company's information systems, a chain of trust agreement defining the terms and conditions of such access must have been signed between the company and the external party.

8. Acceptable Use Policy

The intentions of the Security Team in publishing an Acceptable Use Policy are not to impose restrictions that are contrary to HReasily's established culture of openness, trust and integrity. The Security Team is committed to protecting HRe's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

8.1. Purpose

The purpose of this policy is to outline the acceptable use of computing resources at HReasily. These rules are in place to protect the employee and the company. Inappropriate use exposes HRe to risks including virus attacks, compromise of network systems and services, and legal issues.

8.2. General Use and Ownership

8.2.1. The company's proprietary information stored on electronic and computing devices whether owned or leased by HRe, the employee or a third party, remains the sole property of the company.

8.2.2. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Classification Policy.

8.2.3. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

8.2.4. You may access, use or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned duties. Refer to the Data Classification Policy for more information.

8.2.5. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

8.2.6. Individual departments are responsible for creating guidelines concerning personal use of Internet and Intranet systems.

8.2.7. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

8.2.8. For security and network maintenance purposes, authorized individuals within may monitor equipment, systems and network traffic at any time.

8.2.9. The company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

8.3. Security and Proprietary Information

8.3.1. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

8.3.2. All computing devices must be secured with a **password-protected screensaver** with the automatic activation feature set to **10 minutes or less**.

8.3.3. Never leave your devices unattended in an unsecured location, e.g. in a cafe.

8.3.4. You must **lock the screen or log off when the device is unattended** in a secure location.

8.3.5. You must **password-protect your memory/usb disks** especially those containing confidential and proprietary information.

8.3.6. Postings by employees from a company email address to newsgroups or social media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of business duties.

8.3.7. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

8.4. Unacceptable Use

8.4.1. The following activities in this section, in general, are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job

responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

8.4.2. Under no circumstances is an employee of HRe authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing HRe-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

8.5. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

8.5.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "**pirated**" or other software products that are not appropriately licensed for use by the company.

8.5.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or the end user does not have an active license is strictly prohibited.

8.5.3. Accessing data, a server or an account for any purpose other than conducting business, even if you have authorized access, is prohibited.

8.5.4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

8.5.5. Introduction of malicious programs into the company network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

8.5.6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

8.5.7. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8.5.8. Making fraudulent offers of products, items, or services originating from any company account.

8.5.9. Effecting security breaches or disruptions of network communication.

Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

8.5.10. Port scanning or security scanning (active or passive) is expressly prohibited unless justified with prior notification to the Security Team.

8.5.11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's duties.

8.5.12. Circumventing user authentication or security of any host, network or account.

8.5.13. Introducing honeypots, honeynets, or similar technology on the network unless this activity is done by the Security Team or its delegates.

8.5.14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

8.5.15. Using any program, script or commands, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, by any means, locally or via the internet.

8.5.16. Providing information about, or lists of, employees to external parties without following the proper process in place for such requests.

8.5.17. Providing non-public (i.e. confidential, restricted or internal-use) information to external parties without following the proper process in place for such requests.

8.6. Email and Communication Activities

8.6.1. When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "*the opinions expressed are my own and not necessarily those of the company*" or something similar.

8.6.2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

8.6.3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

8.6.4. Unauthorized use, or forging, of email header information.

8.6.5. Solicitation of email, other than that of the poster's account, with the intent to harass or to collect replies.

8.6.6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

8.6.7. Use of unsolicited email originating from within HRe's networks of other Internet service providers on behalf of, or to advertise, any service hosted by HRe or connected via HRe's network.

8.6.8. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

8.7. Blogging and Social Media

8.7.1. Blogging by employees, whether using HRe's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy.

8.7.2. Limited and occasional use of HRe's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate HRe's policy, is not detrimental to HRe's best interests, and does not interfere with an employee's regular work duties. Blogging from HRe's systems is also subject to monitoring.

8.7.3. Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered when engaged in blogging.

8.7.4. Employees shall not engage in any blogging that may harm, tarnish the image, reputation, and goodwill of any of its employees.

8.7.5. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

8.7.6. Employees may also not attribute personal statements, opinions or beliefs to when engaged in blogging. If an employee is expressing beliefs or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of HRe.

8.7.7. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, HRe's trademarks, logos and any other intellectual property must not be used in connection with any personal blogging activity.

8.7.8. Employees assume any and all risk associated with blogging.

9. Teleworking and Bring-Your-Own-Device (BYOD) Policy

9.1. Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who are connecting a personally-owned device to HRe's organization network for business purposes. The policy applies to any hardware and related software that is not organizationally owned or supplied, but could be used to access organizational resources. That is, devices that employees have acquired for personal use but also wish to use in the business environment.

The overriding goal of this policy is to protect the integrity of the confidential client and business data that resides within HRe's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a device or carried over an insecure network where it could potentially be accessed by unsanctioned resources.

9.2. Scope

This device policy applies, but is not limited to all devices and accompanying media (e.g. USB thumb and external hard drives) that fit the following classifications:

- Laptops, including home desktops
- Smartphones
- Other mobile or cellular phones
- Tablet computers
- Portable media devices
- Any personally-owned device capable of storing organizational data and connecting to a network

The policy addresses a range of threats to enterprise data, or related to its use:

Table 3*: Threats related with BYOD Policy*

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Device Theft	Sensitive or confidential organizational data is deliberately stolen and sold by an employee or unsanctioned third party.
Malware	Ransomware, Viruses, Trojans, worms, spyware, and other threats could be introduced via devices.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the company network and resources.

9.3. Access Control

9.3.1. It is the responsibility of any employee of HRe who uses a personal device to access business resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct HRe business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

9.3.2. The company reserves the right to refuse, by physical and non-physical means, the ability to connect personal devices to company infrastructure and resources. The company will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk.

9.3.3. Prior to initial use on the company infrastructure or resources, all devices must be approved by the company. Devices that are not on this list may not be connected to company infrastructure.

9.3.4. The relevant department will also maintain a list of approved technologies with associated control requirements, if applicable.

9.3.5. End users who wish to connect such devices to non-company network infrastructure to gain access to company data and resources must employ, for their devices and related infrastructure, security measures deemed necessary by the company.

9.3.6. Company data is not to be stored on or accessed from any hardware that fails to meet the company's established security standards.

9.3.7. All personal devices attempting to connect to the company network and resources through the Internet will be inspected using technology centrally managed by the company.

9.3.8. Devices that have not been previously approved, not in compliance with security policies, or represent any threat to the company network or data will not be allowed to connect.

9.3.9. All hosts that are connected to internal networks via remote access technologies or personal workstations that access company resources must use the most up-to-date anti-virus software.

9.3.10. Devices may only access the organizational network and data through the Internet using an IPSec or SSL VPN connection. The SSL VPN portal web address will be provided to users as required.

9.3.11. Smart mobile devices such as smartphones, tablets or the similar devices will access the organizational network and data using mobile VPN software installed on the device by the relevant department.

9.4. Security

9.4.1. Employees using personally-owned devices and related software for network and data access will, without exception, use secure data management procedures.

9.4.2. Any non-business computers used to synchronize with the company network and resources must have up-to-date anti-virus and anti-malware software.

9.4.3. All devices that are able to store data must be protected by a strong password

9.4.4. All data stored on the device must be encrypted using strong encryption (e.g. Full Disk Encryption). See the company's Cryptographic Guidelines for more information.

9.4.5. Employees are never to disclose their passwords to anyone, including family members, or store passwords on personally owned devices.

9.4.6. All users of personally-owned devices must employ reasonable physical security measures. End users are expected to secure all such devices whether or not they are actually in use or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain company data.

9.4.7. Passwords and other confidential data as defined by the company are not to be stored unencrypted on mobile devices.

9.4.8. Any device that is being used to store company data must adhere to the authentication requirements of the company.

9.4.9. The relevant department will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an

intrusion attempt and will be dealt with in accordance with HRe's overarching security policy.

9.4.10. Employees, contractors, and temporary staff will follow all company-sanctioned data removal procedures to permanently erase company-specific data from such devices once its use is no longer required.

9.4.11. In the event of a lost or stolen device, the user must report the incident to the IT department immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than the IT team. Appropriate steps will be taken to ensure that company data on or accessible from the device is secured - including remote wiping of the device where appropriate. The remote wipe may destroy all data on the device, whether it is related to company business or personal.

9.4.12. Employees, contractors, and temporary staff will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system or "jail-breaking") without the express approval from the relevant departments (i.e. IT and Security Team).

9.5. Organizational Protocol

9.5.1. Relevant departments, such as the IT or Security team, must establish audit trails, which will be accessed, published, and used without prior notice.

9.5.2. Such audit trails should be able to track the attachment of an external device to the company network or software running in devices and the resulting reports may be used for investigation of possible breaches or misuse.

9.5.3. The employees agree to and accept that their access and connection to company networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity.

9.5.4. This monitoring is necessary in order to identify accounts or computers that may have been compromised by external parties.

9.5.5. The employee agrees to immediately report to the manager and company's IT department any incident or suspected incidents of unauthorized data access, data loss, or disclosure of company resources, databases, networks, etc.

9.5.6. While a personally-owned device user will not be granted access to organizational resources without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

9.5.7. By signing this policy, employees acknowledge that they fully understand the risks and responsibilities of the BYOD program.

10. Password Policy

10.1. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords. This policy was not created to focus on the password itself, but the overall goal of what a password is. Passwords provide strong user authentication and help to keep attackers out of systems. However, even the strongest password requires other protections to be in place to be most effective (e.g. Multi-Factor Authentication (MFA), account lockouts, account monitoring, etc).

The overall goal of an effective password policy is to allow users to easily make reasonably hard to guess passwords for system access and then monitor and limit access attempts to detect/prevent misuse.

10.2. Authentication Methods

10.2.1. Multi-factor authentication (MFA) should be the first choice for all authentication purposes.

10.2.2. MFA should be enabled for administrator access or other privileged accounts, if supported. MFA, in general, does not make password policy irrelevant, since implementing MFA can be a technical challenge that many systems do not support.

10.2.3. In general, authentication methods rank from best to worst as follows:

10.2.3.1. **MFA**: This should be the goal for all user authentication where possible.

10.2.3.2. **Password Manager**: These tools generate and store unique lengthy/complex passwords per account, and can greatly increase the security and usability of passwords when supported.

10.2.3.3. **Human generated/remembered passwords**: This method is not going away anytime soon and is the most common authentication method.

10.3. General Policies

10.3.1. All passwords are to be treated as sensitive and confidential HReasily information.

10.3.2. Password Creation

10.3.2.1. All user-level and system-level passwords must conform to the Password Construction Guidelines.

10.3.2.2. Users must use a separate, unique password for each of their work related accounts.

10.3.2.3. Users must not use any work related passwords for their personal accounts or vice versa.

10.3.2.4. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. Use multi-factor authentication for any privileged accounts, if applicable.

10.3.3. Password Length - Password Only Account

10.3.3.1. In cases where a password is the only authentication on a given account, use a minimum length to 14 characters

10.3.3.2. Use passphrases for longer and more secure passwords.

10.3.3.3. Maximum length should be as long as possible based on system constraints.

10.3.3.4. This type of account should be targeted to migrate to using MFA and away from password-only authentication where possible.

10.3.4. Password Length - MFA Account: Password as a Factor

10.3.4.1. In cases where a password is used as one of the factors in an MFA system, use the 8-character minimum length.

10.3.4.2. Maximum length should be as long as possible based on system constraints.

10.3.5. Password Complexity - Password Only Account

10.3.5.1. Allow any character to be included in the password and require at least one non-alphabetic character (Number or “Special Character”).

10.3.6. Password Complexity - MFA Account: Password as a Factor

Allow any character to be included in the password with no complexity requirement.

10.3.7. Password Change or Rotation - For user-related passwords

10.3.7.1. Change based on events including but not limited to:

- Indication of compromise
- Change of user role

- Off-boarding a user (when a user leaves the company)

10.3.7.2. Implement a yearly password change

10.3.8. Password Change or Rotation - For service-accounts or other shared-accounts

10.3.8.1. Always change the default password

10.3.8.2. Change or rotate passwords based on events including but not limited to:

- Indication of compromise

10.3.8.3. Implement password rotation with a frequency that is based on some decision-making practice such as a risk assessment (e.g. every year)

10.3.9. Password Protection

Passwords must not be shared with anyone, including supervisors and coworkers.

10.3.9.1. Do not reveal a password over the phone to ANYONE

10.3.9.2. Do not reveal a password in an email message

10.3.9.3. Do not reveal a password to the boss or colleague

10.3.9.4. Do not talk about a password in front of others

10.3.9.5. Do not hint at the format of a password (e.g., "my family name")

10.3.9.6. Do not reveal a password on questionnaires or security forms

10.3.9.7. Do not share a password with family members

10.3.9.8. Do not reveal a password to co-workers while on vacation

10.3.9.9. Do not write passwords down and store them anywhere (office, personal workstations, etc)

a. Do not store passwords in a file on ANY computer system or mobile device without encryption

b. Passwords may be stored only in “password managers” authorised by the organization.

c. Do not use the "Remember Password" feature of applications (e.g. web browsers).

d. Passwords must not be inserted into email messages or other forms of electronic communication without encryption.

e. If someone demands a password, refer them to this document or have them call someone from the Security team.

f. Password cracking or guessing may be performed on a periodic or random basis by the Security team or its delegates.

g. If a password is guessed or cracked during one of these scans, the user will be required to change it.

10.3.9.10. The Security team or its delegates may require you to change your passwords in the event that your personal information has been found in public database dumps or pastes containing leaked accounts.

Note: A paste is information that has been published to a publicly facing website designed to share content (e.g. pastebin.com) and is often an early indicator of a data breach.

10.3.10. Best Practices (Optional Implementation)

10.3.10.1. Password Managers

a. Encouraging the use of an approved password manager lets users create strong passwords that are not reused on multiple systems.

b. Use of these should be actively encouraged for use with password-only authentication systems (especially if
the user needs to manage access to multiple of these systems).

c. Where feasible, using MFA instead of just a master password to gain access to the Password Manager is preferred.

10.4. Application Development

10.4.1. General

10.4.1.1. Applications must support authentication of individual users, not groups.

10.4.1.2. Applications must not store passwords in clear text or in any reversible form. Follow NIST Special Publication 800-175B - see Cryptographic Standards Guidelines for a summary of the publication.

10.4.1.3. Applications must not transmit passwords in clear text over the network.

10.4.1.4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

10.4.2. Session lock when idle

10.4.2.1. Lock the user system or current session after a reasonable amount of time (e.g. 15 minutes) of being idle (i.e. no user input).

10.4.2.2. The Session Lock login should be the same type as normal account login.

10.4.3. Limit failed login attempts (lockout)

10.4.3.1. To limit password guessing, temporarily lock the account after a predefined number of failed login attempts. The overall goal is it to make it difficult for an attacker to guess a password by trying it against an account, while allowing a user the ability to correct a mistakenly entered password in a reasonable way, e.g.

a. temporary account lockout (15 minutes or more) after five consecutive failed attempts, or

b. time doubling throttling (in minutes) between each retry (0, 1, 2, 4, 8, etc.) with a permanent account lockout (IT reset required) after 12 retries.

10.4.3.2. Monitor failed login attempts, at minimum:

a. Log all failed attempts

b. Alert key personnel when a temporary or permanent account lockout has been triggered

c. Log and alert key personnel about login attempts from unexpected geographical area

d. Log and alert key personnel about login attempts at unexpected times

e. If the organisation employed "honeypot accounts", log and alert key personnel about login attempts on these accounts

10.4.4. Suspend accounts on non-use

10.4.4.1. Unused accounts should be turned off, if practical, disabling of unused accounts should be automatic

10.4.4.2. Suspend accounts after a certain number of days based on without a valid login; e.g. automatically suspend the account after 45 days without a valid login

10.4.5. Best Practices (Optional Implementation)

10.4.5.1. Password Strength Indicators on Creation

a. Strength indicators are helpful, since most people want to make a strong password.

b. When creating a new password, the system should offer guidance to the user, such as a password-strength indicator, to assist the user in creating a strong password.

c. Strength indicators have been shown to increase password strength, and decrease user frustration when creating a new password.

10.4.5.2. On Password Display: There are two main use cases for password display:

a. On Password Creation: Allowing a user to display their password on creation is better than a confirmation field. To assist the user in creating a password, the system should offer an option to display the password, instead of a series of dots or asterisks, until they enter it. This allows the user to verify their entry if they are in a location where their on-screen password is unlikely to be seen. This works much better than a blind confirmation field for mistyped passwords.

b. On Password Use: Allowing a user to briefly see what they are typing in a password field reduces entry errors. The system should optionally permit the user's device to display individual entered characters for a short time after they type each character to verify correct entry (then replaced with an asterisk or dot). This can be particularly useful on mobile devices where the text fields are small and hard to see.

10.4.5.3. Allow Paste

a. It is recommended that systems permit users to use the paste functionality when entering a password, since this facilitates the use of password managers.

b. Using a password manager is much more secure even if paste needs to be enabled for some application(s) to work properly.

11. Server Security Policy

For the purposes of this document, “servers” refers to physical, logical or virtual servers that are built, hosted and delivered to serve HReasily customers and employees.

11.1. General Requirements

11.1.1. All internal servers deployed for HReasily must be owned by an operational group that is responsible for system administration.

11.1.2. Approved server configuration guides must be established and maintained by each operational group, based on business needs. Approval is based on **Review Process**.

11.1.3. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval based on **Review Process**.

11.1.4. The following items must be met:

11.1.4.1. Servers must be registered within the organisation’s management system. At a minimum, the following information is required:

a. Server contact(s) and location, and a backup contact

b. Hardware and Operating System/Version

c. Main functions and applications, if applicable

d. Identification of critical assets

e. Identification if the asset contains *personal data*.

11.1.4.2. Information in the corporate enterprise management system must be kept up-to-date.

11.1.4.3. Configuration changes for production servers must follow the appropriate **Review Process**

11.1.4.4. For security, compliance, and maintenance purposes, only authorized users are allowed to monitor and audit equipment, systems, processes, and network traffic.

11.2. Services, Applications and Integrations

11.2.1. All services, applications and integrations must be owned by an operational group that is responsible for its administration.

11.2.2. Approved server configuration guides must be established and maintained by each operational group, based on business needs. Approval is based on the **Review Process**.

11.2.3. Services must be registered within the organisation's management system. At a minimum, the following information is required:

11.2.3.1. Server contact(s) and location, and a backup contact

11.2.3.2. Hardware and Operating System/Version, if applicable

11.2.3.3. Main functions and applications, if applicable

11.2.3.4. Identification of critical assets

11.2.3.5. Identification if the asset contains *personal data*. See additional *Personal Data Protection Policy* for such assets.

11.2.4. Configuration should be in accordance with approved security guidelines.

11.2.5. Where applicable, services should be subject to hardening guidelines as provided by the vendor, insofar as these do not interfere with desired functions or access.

11.2.6. Services, applications and integrations that will not be used must be disabled where practical.

11.2.7. A documented list of services, applications and integrations should be maintained and reviewed regularly (e.g. software asset inventory).

11.2.8. Access to services should be logged and/or protected through access-control methods.

11.2.9. Business-critical services and applications should have multi-factor authentication methods in place. (e.g. enforcement of Second-factor Verification for Google accounts)

11.2.10. Access to critical services should be logged, protected and monitored.

11.2.10.1. e.g. Critical systems storing confidential data should be protected by firewalls with the bare minimum of ports opened only to those sources that should access them.

11.2.11. Critical services and applications should have a documented and successfully tested backup policy in place.

11.2.12. The most recent and critical security patches must be installed on the system as soon as practical and reasonable. Immediate application of security patches is ideal unless this interferes with business requirements. For such cases, a reasonable expectation of delay is justified.

11.2.13. Regular preventive maintenance (security and/or system patches) should be carried out monthly.

11.2.14. Zero-trust environment

11.2.14.1. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

11.2.15. Principle of Least Privilege

11.2.15.1. Always use standard security principles of least required access to perform a function.

11.2.15.2. Do not use root when a non-privileged account will do.

11.2.15.3. Maintain an updated list of user access and permissions. This list should be reviewed regularly.

11.2.16. Service accounts

11.2.16.1. Passwords should be saved and shared only through a password management system. These should be rotated based on the defined **Password Policy** or when off-boarding users with admin access.

11.3. Infrastructure Security

11.3.1. Privileged access must be performed over secure channels where technically feasible e.g. encrypted network connections using SSH or IPSec

11.3.2. ***AWS Key Pairs***: Generate your AWS key pairs securely based on AWS best practices. E.g. generate using OpenSSL in a secure and trusted workstation or generate the keys from AWS itself

11.3.3. Perform vulnerability and compliance scans as frequently as needed

11.3.4. AWS Security Groups should be limited to only required flows (inbound and outbound)

11.3.5. All internet-facing applications should be protected by a fully-working and active protection mechanisms such as Web Application Firewall (WAF), Intrusion Detection/Prevention Systems, etc.

11.3.6. Fine-tuning of device rules for optimal performance should be conducted regularly.

11.3.7. All external applications such as FTP should be restricted by whitelisting IPs. If this is not possible, the risk must be documented and accepted in the risk register.

11.3.8. All management services (e.g. SSH) should not be exposed to the Internet.

11.3.9. Private resources must be in a private subnet with Internet access only provided via Nat Gateway

11.4. Monitoring and Incident Response

11.4.1. Ensure that security controls are in place for the emergency privileged (break-glass) account. This account should be tightly monitored.

11.4.2. If applicable, logs all commands executed on the production and/or critical hosts to be reviewed by the security team.

11.4.3. All security-related events on critical or sensitive systems must be logged and audit trails based on the **Backup Policy**.

11.4.4. Security-related events will be reported to the Security team, who will review logs and raise security incidents as per **Incident Handling Process**. Corrective measures will be prescribed as needed. This process should be documented in the **Vulnerability Management Process**.

11.4.5. Security-related events include, but are not limited to:

11.4.5.1. Port-scan attacks
11.4.5.2. Evidence of unauthorized access to privileged accounts
11.4.5.3. Anomalous occurrences that are not related to specific applications on the host.

11.4.6. Runbooks have been developed and documented for common incident events

11.4.7. Incident alerting thresholds are established

11.4.8. Business Continuity Plans should be well documented and regularly tested

11.5. AWS Cloud Server Security Policy

11.5.1. Unless approved with documented justification, HReasily does not maintain physical servers in any of the offices or datacenter.

11.5.2. The servers are provisioned only through our Cloud provider: AWS.

11.5.3. Asset Management

11.5.3.1. Ensure accurate inventory of all AWS accounts, systems, and resources.

11.5.3.2. All accounts must have accurate account contact information (billing, operations, security). Refer to the General Requirements in this document.

11.5.3.3. All accounts must be enrolled in the AWS Organization structure for centralized management

11.5.4. Identity & Access Management

11.5.4.1. Ensure only authenticated and authorised individuals have the ability to interact with AWS resources.

11.5.4.2. Federation of identity is ideal but not compulsory. Federation means that instead of AWS IAM user accounts - single sign-on such as AWS SSO, Third-Party (Okta, Ping Identity) or On-Premises Identity Provider is implemented.

11.5.4.3. All console access must have multi-factor authentication enforced
Strong password policy must be enforced.

11.5.4.4. Long term access keys should be replaced with temporary credentials (IAM Assume Role)

11.5.4.5. Long term access keys if required should be rotated per the Password Rotation Policy

11.5.4.6. Users should have their own accounts. No shared user accounts are allowed.

11.5.4.7. Users should have permissions appropriate for their job role - *see **Principle of Least Privilege** control in this document*

11.5.5. Detective Controls

11.5.5.1. Ensure the ability to detect malicious or non-compliant actions across the AWS platform

11.5.5.2. Centralize all logs and review and action on alerts

11.5.5.3. Leverage and integrate Trusted Advisor findings

11.6. Risk Register

11.6.1. If controls are not technically practical (e.g. due to business requirements), the risk, controls and mitigation measures must be properly documented in the risk register and accepted by management.

11.7. Risk Assessments and Reviews

11.7.1. Risk assessments and management review sessions should be conducted annually. Risk assessment reports and records of meeting minutes should be documented and stored.

11.8. Items to Audit, Review and Rotate

11.8.1. Validate the controls specified in this policy by performing audit or review of such items.

11.8.2. Approval workflow is based on **Review Process**.

11.8.3. The audit and/or review of the above items should be scheduled promptly and performed judiciously.

12. Backup Policy

12.1. Backup Strategy

12.1.1. Employ redundancy in critical infrastructure where business services and applications are hosted.

12.1.2. Whatever backup strategy is employed depends on the data classification, technical limitations and business needs.

12.1.3. The best time to backup is whenever data changes.

12.1.4. Most backup systems work by backing up all of your data once (full), or incrementally updating only what's changed or new (differential backups).

12.1.5. Taking snapshots of the data as backup on a certain predefined frequency may also be used.

12.1.6. Also consider creating backup of your backup for redundancy.

12.1.7. Depending on the technical practicality and business need, there may be a need to rotate backups periodically to make sure that even if one backup fails, another can take its place

12.2. Data Backup Procedures

12.2.1. Any data that's critical to keeping your business running should be backed up. e.g. Financial records, customer records, tax forms, sales records, policies, source code, software, and project plans

12.2.2. Each team should identify all sensitive data that needs to be maintained and backed up.

12.2.3. Critical data MUST be encrypted at rest according to the best and most practical encryption method available. See Cryptographic Standards Guidelines for more information on the appropriate levels of protection according to the sensitivity level.

12.2.4. Access to confidential, sensitive and critical files should be controlled through access control procedures. See Access Control Policy

12.3. Backup Schedule

12.3.1. Critical backups should be scheduled. See Summary of Scheduled Controls

13. Disaster Contingency Policy

13.1. Business Continuity vs Disaster Recovery

Business continuity: Strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level

Disaster recovery: The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster

The focus of disaster recovery (DR) is on technology while business continuity (BC) is on business operations. The Disaster Recovery Plan (DRP) is an enabler of Business Continuity Plan (BCP) as it is the technological counterpart of the BCP.

13.2. Incident vs Disaster

Incident: A situation that might be, or could lead to, a disruption, loss, emergency or crisis

Disaster: Any event that has a negative impact on the business continuity or finances. This could be hardware or software failure, a network outage, a power outage, physical damage to a building like fire or flooding caused by adverse weather conditions, human error, or some other significant disaster that impacts business operations.

Therefore, an event can lead to an incident, and an incident can result in a disaster.

This policy requires management to financially support and diligently attend to disaster contingency planning efforts, this includes business continuity planning efforts and disaster recovery efforts.

13.3. Purpose

This policy defines the requirement for a baseline disaster contingency planning efforts: business continuity and disaster recovery plan.

The business continuity plan is to be developed and implemented by the business operations team. The disaster recovery plan is to be developed and implemented by the Technical operations team that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

13.4. Scope

This policy defines the requirement for a baseline disaster contingency planning efforts: business continuity and disaster recovery plan.

This policy is directed to the Business Units who are accountable to ensure that the BCP is developed, tested and kept up-to-date. This is also directed to the Technical operations team who is accountable to ensure the DRP is developed, tested and kept up-to-date.

This policy is solely to state the requirement to have a business continuity plan and disaster recovery plan, it does not provide requirements around what goes into the plan or sub-plans.

13.5. General

13.5.1. The organisation should create, maintain and operate disaster contingency plans.

13.5.2. These plans include the creation of a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP).

13.5.3. The Business units are accountable to the creation, maintenance, testing and review of the BCP.

13.5.4. The BCP is encouraged to follow the industry standard such as ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements. Guidance on this standard is reflected in ISO 22313:2020.

13.5.5. The Technical operations team is accountable to the creation, maintenance, testing and review of the DRP.

13.5.6. The following contingency plans must state the following:

13.5.6.1. Response

a. Who is to be contacted, when, and how?

b. What immediate actions must be taken in the event of certain occurrences?

c. Describe the flow of responsibility when normal staff is unavailable to perform their duties.

d. Data Study

13.5.6.1.d.1. Detail the data stored on the systems including criticality, and confidentiality. Refer to Data Classification Policy.

e. Services

13.5.6.1.e.1. List all the services provided and their order of importance.

f. Data Backup and Restoration

13.5.6.1.f.1. Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done.

13.5.6.1.f.2. It should also describe how that data could be recovered.

13.5.6.1.f.3. Explain the order of recovery in both short-term and long-term timeframes. See Backup Policy.

13.6. Testing and Review

13.6.1. The plans should be tested and reviewed.

13.6.2. After creating the plans, it is important to practice them to the extent possible.

13.6.3. Management should set aside time to test implementation of the disaster recovery plan.

13.6.4. Management should set aside time to review the disaster recovery plan.

13.6.5. The plan, at a minimum, should be reviewed and updated on an annual basis

13.6.6. Testing or table top exercises should be conducted annually.

13.6.7. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

13.6.8. Record of tests and reviews must be kept.

14. Data Breach Response Policy

14.1. Purpose

HRe Security Team's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how HRe's established culture of openness, trust and integrity should respond to such activity.

14.2. Definition of Terms

Event: Anything that has happened

Incident: A security event that compromises the C-I-A of an information asset

Breach: An incident that results in the confirmed disclosure (not just potential exposure) of data to unauthorised party

Encryption or encrypted data: The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text: Unencrypted data.

Hacker: A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Personally Identifiable Information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

Protected data: See PII and PHI

Information Resource: The data and information assets of an organization, department or unit.

Safeguards: Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data: Data that is encrypted or in plain text and contains PII data. See PII above.

14.3. General Policies

14.3.1. A procedure for receiving and responding to personal data complaints should be established. This procedure should be available to the public.

14.3.2. As a data controller

14.3.2.1. Once HReasily has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), the organisation is to take reasonable and expeditious steps to assess whether the data breach is **notifiable** under the relevant governing authority.

14.3.2.2. Assessments should be done expeditiously as the likelihood of significant harm to affected individuals may increase with time.

14.3.2.3. Under Singapore's Personal Data Protection Act, any unreasonable delay in assessing a data breach will be a breach of the Data Breach Notification Obligation (Part VIA) and the Personal Data Protection Commission (PDPC) can take enforcement action.

14.3.2.4. The organisation should complete the investigation (facts of the breach and whether it is notifiable) within 30 calendar days. If HReasily is unable to complete its assessment within 30 calendar days, the DPO, on behalf of HReasily, should inform the regulatory body with an explanation for the time taken to carry out the assessment.

14.3.3. As a data intermediary

14.3.3.1. Once HReasily has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), HReasily, in its capacity as a data intermediary, is required to notify the business customers without undue delay from the time it has credible grounds to believe that the data breach has occurred.

14.3.3.2. This ensures the business customers are (a) informed of data breaches in a timely way; (b) able to decide on the immediate actions to take to contain the data breach; and (c) able to assess whether the data breach is a notifiable data breach.

14.3.3.3. HReasily, as a data intermediary, should assist our business customers in conducting the assessment of the data breach if it falls under our purview.

14.3.3.4. We should establish clear procedures for complying with the data breach notification obligation (if relevant) when entering into service agreements or contractual arrangements with our business customers.

14.3.3.5. These agreements take into consideration factors relating to the data processing, such as the volume and types of personal data involved, the type and extent of data processing, and the potential harm that may result from a data breach.

14.3.4. Documentation of the data breach

14.3.4.1. The steps taken in assessing the data breach should be documented.

14.3.4.2. To ensure proactive steps are taken by the organisation to manage and remediate the data breach, information to be provided in HReasily's notification to the **relevant governing body** shall include:

a. Facts of the data breach

14.3.4.2.a.1. the date on which and the circumstances in which the organisation first became aware that a data breach has occurred;

14.3.4.2.a.2. information on how the notifiable data breach occurred;

14.3.4.2.a.3. the number of affected individuals affected by the notifiable data Breach;

14.3.4.2.a.4. the personal data or classes of personal data affected by the notifiable data breach; and

14.3.4.2.a.5. the potential harm to the affected individuals as a result of the notifiable data breach.

b. Data breach handling

14.3.4.2.b.1. A chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment that the data breach is a notifiable data breach;

14.3.4.2.b.2. information on any action by the organisation, whether taken before or to be taken after the organisation notifies the regulatory body of the occurrence of the notifiable data breach:

14.3.4.2.b.2.1. to eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and

14.3.4.2.b.2.2. to address or remedy any failure or shortcoming that the organisation believes to have caused, or have enabled or facilitated the occurrence of, the notifiable data breach; and

14.3.4.2.b.3. information on the organisation's plan (if any) to inform all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach. The organisation may provide in general terms the steps taken or intended to be taken.

c. Contact details

14.3.4.2.c.1. Contact details of at least one authorised representative of the organisation. The representative(s) need not be the organisation's DPO (or a person assuming the DPO's responsibilities in the organisation).

14.3.4.2.c.2. Where the data breach notification to the relevant governing authority is not made within three (3) calendar days of ascertaining that it is a notifiable breach, the organisation must also specify the reasons for the late notification and include any supporting evidence.

14.3.4.2.c.3. Where the organisation does not intend to notify any affected individual, the notification to the relevant governing body must additionally specify the grounds (whether under any relevant governing written law) for not notifying the affected individual.

14.3.4.2.c.4. Any application to the relevant governing authority to waive the requirement to notify an affected individual may be submitted together with the notification.

14.3.5. Notification of Data Breach

14.3.5.1. On determining that a data breach is notifiable, HReasily must notify:

a. the relevant governing authority as soon as practicable, but in any case, no later than three (3) calendar days; and

b. where required, affected individuals as soon as practicable, at the same time or after notifying the relevant governing authority.

14.3.5.2. **An exception may apply to notify individuals** to a data breach that is likely to have significant harm to the affected individuals or if prohibited by law. Although HReasily need not notify the affected individuals, but it is still required to notify the relevant governing authority of the data breach.

14.3.5.3. If required to notify affected individuals of a data breach, the mode of notification to be used should be appropriate and effective in reaching the affected individuals in a timely way.

14.3.5.4. Notification to affected individuals should be clear and easily understood. It should include guidance on the steps affected individuals may take to protect themselves from the potential harm arising from the data breach.

14.3.5.5. HReasily should include the following information in the notification to **affected individuals**:

a. Facts of the data breach

14.3.5.5.a.1. the circumstances in which HReasily first became aware that a notifiable data breach has occurred; and

14.3.5.5.a.2. (the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach.

b. Data breach management and remediation plan

14.3.5.5.b.1. Potential harm to the affected individual as a result of the notifiable data breach;

14.3.5.5.b.2. Information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual

14.3.5.5.b.2.1. to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach;

14.3.5.5.b.2.2. To address or remedy any failure or shortcoming that the organisation believes to have caused, or have enabled or facilitated the occurrence of, the notifiable data breach; and

14.3.5.5.b.3. Steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the affected individual's personal data affected by the notifiable data breach.

c. Contact details

14.3.5.5.c.1. Contact details of at least one authorised representative whom the affected individual can contact for further information or assistance. The representative(s) need not be the organisation's DPO (or a person assuming the DPO's responsibilities in the organisation), or the same representative provided in the organisation's notification to the relevant governing authority.

14.3.6. Confirmed theft, data breach or exposure of HRe Protected/Sensitive data

14.3.6.1. As soon as a theft, data breach or exposure containing HRe Protected data or Sensitive data is identified, the process of removing all access to that resource will begin.

14.3.6.2. The Executive Director (CEO or CTO) will chair an incident response team to handle the breach or exposure.

14.3.6.3. The team will include members from:

- Head of Department or Data Protection Officer (if it's a data/privacy breach)
- IT Infrastructure
- Finance (if applicable)
- Legal
- Marketing and Communications (Press and Public Relations)
- Customer Success
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved,
- Additional individuals as deemed necessary by the Executive Team

14.3.7. Confirmed theft, breach or exposure of HRe data

14.3.7.1. The Executive Director will be notified of the theft, breach or exposure. The Engineering Department, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

14.3.8. Work with Forensic Investigators

14.3.8.1. As provided by HRe cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals

and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

14.3.9. Develop a communication plan

14.3.9.1. Work with HRe communications, legal and human resource departments to decide how to communicate the breach to:

a. internal employees,
b. the public, and
c. those directly affected

14.3.10. Ownership and Responsibilities

14.3.10.1. Sponsors: Members of the HRe community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any HRe Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

14.3.10.2. Information Security Administrator: Member of the HRe community, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

14.3.10.3. Users: All members of the HRe community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

14.3.10.4. The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives:

a. Security Team
b. Infrastructure
c. Application Security
d. Communications
e. Legal
f. Management
g. Financial Services
h. Member Services
i. Human Resources

15. Security Response Policy

15.1. The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation with the Security Team.

15.2. Business units are expected to properly facilitate the SRP applicable to the service or products they are held accountable for. The business unit coordinator or product owner is further expected to work with the Security team in the development and maintenance of a Security Response Plan.

15.3. Service or Product Description

15.3.1. The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

15.4. Contact Information

15.4.1. The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required.

15.4.2. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to the customer.

15.4.3. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

15.5. Triage

15.5.1. The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

15.6. Identified Mitigations and Testing

15.6.1. The SRP must include a defined process for identifying and testing mitigations prior to deployment.

15.6.2. These details should include both short-term mitigations as well as the remediation process.

15.7. Mitigation and Remediation Timelines

15.7.1. The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company.

15.7.2. These response guidelines should be carefully mapped to the level of severity determined for the reported vulnerability.

16. Personal Data Protection Policy

16.1. Definition of Terms

PDPA: Singapore Personal Data Protection Act 2012 (**PDPA**) **is** a law that governs the collection, use and disclosure of personal data by all private organisations. The Act has come into full effect on 2nd July 2014 and has been updated recently with new amendments that take effect on 2 November 2020.

Regulatory body: A government office, committees or officers with vested functions under the law in a country or territory with respect to the enforcement or the administration of provisions of the law of that country or territory concerning personal data.

For example: Personal Data Protection Commission in Singapore, National Data Protection Authority in Hong Kong, National Privacy Commission in The Philippines, Personal Data Protection Commissioner in Malaysia, and Personal Data Committee in Thailand

Individuals: a natural person, whether living or deceased.

The term “natural person” refers to a human being. This may be distinguished from juridical persons or “legal persons” which are other entities that have their own legal personality and are capable of taking legal action in their own name. An example of such a “legal person” is a body corporate such as a company. The term “natural person” would also exclude unincorporated groups of individuals such as an association which may take legal action in its own name.

Only the personal data of natural persons is protected under the PDPA. Data relating to corporate bodies and other entities are not covered.

Personal data: data, whether true or not, about an individual who can be identified —

a) from that data; or

b) from that data and other information to which the organisation has or is likely to have access.

Data about an individual

Data about an individual includes any data that relates to the individual. Some examples of data that is about an individual include information about an individual's health, educational and employment background, as well as an individual's activities such as spending patterns.

Not all data that relates to an individual may identify the individual. For example, a residential address, on its own, relates to a particular place and there could be several individuals residing there. Hence, whether a residential address constitutes personal data would depend on whether the address is associated with a particular identifiable individual so as to form part of the individual's personal data.

Individual who can be identified

Data constitutes personal data if it is data about an individual who can be identified from that data on its own, or from that data and other information to which the organisation has or is likely to have access.

Certain types of data can, on its own, identify an individual, for instance biometric identifiers which are inherently distinctive to an individual, such as the face geometry or fingerprint of an individual.

Data that has been assigned to an individual for the purposes of identifying the individual (e.g. NRIC or passport number of an individual) would be able to identify the individual from that data alone.

Such data which, on its own, constitutes personal data, is referred to as a "unique identifier" in these guidelines. Data that the regulatory body generally considers unique identifiers include:

- Full name
- NRIC Number or FIN (Foreign Identification Number)
- Passport number
- Personal mobile telephone number
- Facial image of an individual (e.g. in a photograph or video recording)
- Voice of an individual (e.g. in a voice recording)
- Fingerprint
- Iris image
- DNA profile

Individual can be identified from that data and other information to which the organisation has or is likely to have access

Generic information, such as gender, nationality, age or blood group, alone is not usually able to identify a particular individual (e.g. gender alone cannot identify the individual). Nevertheless, such information may

constitute part of the individual's personal data if it is combined with a unique identifier or other information such that it can be associated with, or made to relate to, an identifiable individual.

Excluded personal data

The PDPA does not apply to the following categories of personal data:

a) Personal data that is contained in a record that has been in existence for at least 100 years; and

b) Personal data about a deceased individual who has been dead for more than 10 years.

For personal data about a deceased individual who has been dead for 10 years or less, the PDPA applies to a limited extent. For such personal data, only the provisions relating to the disclosure and protection of personal data will apply.

Sensitive personal data

Information relating to the physical or mental health or condition, political opinions, religious belief or other beliefs of a similar nature.

e.g. records of individuals with HIV, records of adopted children and their biological parents

Publicly available personal data

Refers to personal data (about an individual) that is generally available to the public, including personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

Business contact information

The Data Protection Provisions do not apply to business contact information.

Business contact information is defined in the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".

Organisations are not required to obtain consent before collecting, using or disclosing any business contact information or comply with any other obligation in the Data Protection Provisions in relation to business contact information.

The definition of business contact information is dependent on the purpose for which such contact information may be provided by an individual as it recognises that an individual may provide certain work-related contact information solely for personal purposes.

In such situations, the information would not constitute business contact information and organisations would be required to comply with the Data Protection Provisions in respect of such information.

Organisation**:** any individual, company, association or body of persons, corporate or unincorporated whether or not formed or recognised under the law of Singapore; or resident, or having an office or a place of business, in Singapore.

Every organisation is required to comply with the PDPA in respect of activities relating to the collection, use and disclosure of personal data in Singapore unless they fall within a category of organisations that is expressly excluded from the application of the PDPA.

An organisation should ensure that it is able to adduce evidence to establish and demonstrate that it complied with the obligations under the PDPA in the event of an investigation.

Data intermediary: an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation

A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities which do not constitute processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

Determination on who the data intermediary is

An organisation may be a data intermediary of another even if the written contract between the organisations does not clearly identify the data intermediary as such. The PDPA's definition of "data intermediary" would apply in respect of all organisations that process personal data on behalf of another.

Hence it is very important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, **include provisions in their written contracts to clearly set out each organisation's responsibilities and liabilities** in relation to the personal data in question including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation.

- It is possible for an organisation that is part of a corporate group of organisations to act as a data intermediary for other members of the group.
- An organisation can be considered a data intermediary in respect of a set of personal data while at the same time be bound by all Data Protection Provisions in relation to other sets of personal data.

Purpose: The term "purpose" does not refer to activities which an organisation may intend to undertake but rather to its **objectives or reasons**. Hence, when specifying its purposes relating to personal data, an organisation is not required to specify every activity which it may undertake, but its objectives or reasons relating to personal data.

16.2. Policy

16.2.1. Lawful, fair and transparent processing

16.2.1.1. To ensure its processing of data is lawful, fair and transparent, HReasily shall maintain a Register of Systems.

16.2.1.2. The Register of Systems shall contain the following:

a. The data we collect and in what way

b. How the data are stored and who has access to them

c. Sharing the data

d. Purpose for which the data are used

e. Data retention (removal and archiving)

f. Lawful purpose

16.2.1.3. The Register of Systems shall be reviewed at least annually.

16.2.1.4. Individuals have the right to access their personal data and any such requests made to the organisation shall be dealt with in a timely manner.

16.2.1.5. Access requests shall be documented.

16.2.2. Lawful purposes

16.2.2.1. All data processed by the organisation must be done on one of the following lawful bases: consent, deemed consent (notification, legitimate interest, business improvement and research) , contract, legal obligation, vital interests or public task.

16.2.2.2. Reliance of the organisation in the collection, use and disclosure of personal data for any of the purposes in which the consent is deemed should undergo risk assessment. This assessment shall be documented. When necessary and required by law, reliance on this consent shall be made available to the users.

16.2.2.3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent, except when it falls under deemed consent by notification, shall be documented.

16.2.2.4. Where communications are sent to individuals based on their consent, the option for the individual to withdraw their consent should be clearly available and

systems should be in place to ensure such withdrawal is reflected accurately in the HReasily systems.

16.2.3. Data minimisation

16.2.3.1. The organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

16.2.4. Accuracy

16.2.4.1. The organisation shall take reasonable steps to ensure personal data is accurate.

16.2.4.2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

16.2.5. Data retention

16.2.5.1. To ensure that personal data is kept for no longer than necessary, the organisation shall put in place a data retention policy for each area in which personal data is processed and review this process annually.

16.2.5.2. The data retention policy shall consider what data should be retained, for how long, and why.

16.2.6. Security

16.2.6.1. The organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

16.2.6.2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

16.2.6.3. When personal data is deleted or anonymised - this should be done safely such that the data is irrecoverable.

16.2.6.4. Appropriate back-up and disaster recovery solutions shall be in place.

16.2.7. Breach

16.2.7.1. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the appropriate regulatory body.

16.3. Data intermediaries

16.3.1. Obligations of data intermediaries

16.3.1.1. The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Data Protection Provisions relating to:

(a) protection of personal data (later referred to as the "Protection Obligation");

(b) retention of personal data (later referred to as the "Retention Limitation Obligation"); and

(c) notifying the organisation of data breaches as part of notification of data breaches (later referred to as the "Data Breach Notification Obligation"),

and not any of the other Data Protection Provisions.

A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities which do not constitute processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

16.3.2. Considerations for organisations using data intermediaries

16.3.2.1. Section 4(3) of the PDPA provides that the organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data were processed by the organisation itself.

16.3.2.2. HReasily must undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with the PDPA.

a. The due diligence can be in the form of a risk or vendor assessment, a checklist or some other industry standard form of documentation.

16.3.2.3. When engaging a data intermediary, the organisation should make clear in its contract the scope of work that the data intermediary is to perform on its behalf and for its purposes.

For instance, if the organisation requires the data intermediary to process personal data on its behalf to respond to access or correction requests by individuals, the organisation should include contractual clauses to ensure that the data intermediary's scope of work and level of responsibilities are clear.

16.3.2.4. The data intermediary has independent obligations to protect and cease retention of personal data that it has received for processing under the contract.

16.3.2.5. Where a data breach is discovered by a data intermediary that is processing personal data on behalf and for the purposes of another organisation, the data intermediary is required to notify the organisation without undue delay from the time it has credible grounds to believe that the data breach has occurred.

16.3.2.6. HReasily remains liable for any breach of the Data Protection Provisions for any processing by a data intermediary on its behalf and for its purposes.

16.3.3. Scope on contractual clauses

16.3.3.1. In setting out contractual clauses that require the recipient to comply with a standard of protection in relation to the personal data transferred to him that is at least comparable to the protection under the PDPA, HReasily, as a transferring organisation, should minimally set out protections with regard to the following:

	Area of Protection	Recipient is a data intermediary	Recipient is an organisation (except data intermediary)
1	Purpose of collection, use and disclosure by recipient	N/A	✓
2	Accuracy	N/A	✓
3	Protection	✓	✓
4	Retention Limitation	✓	✓
5	Policies on personal data protection	N/A	✓
6	Access	N/A	✓
7	Correction	N/A	✓

8	Data Breach Notification	✓ To notify organisation of data breaches without undue delay	✓ To assess and notify the regulatory body/affected individuals of data breaches, where relevant

16.4. Cross-border transfer of personal data

16.4.1. Section 26 of the PDPA limits the ability of the organisation (HReasily) to transfer personal data to another organisation outside Singapore in circumstances where it relinquishes possession or direct control over the personal data.

16.4.2. **Such circumstances include transferring personal data to another company within the same group for centralised corporate functions, or to a data intermediary for data processing.**

16.4.3. Where personal data transferred or situated overseas remains in the possession or control of an organisation, the organisation has to comply with all the Data Protection Provisions.

For example, an employee travels overseas with customer lists on his notebook; an organisation owns or leases and operates a warehouse overseas for archival of customer records; or an organisation stores personal data in an overseas data centre on servers that it owns and directly maintains.

In the above examples, the organisation has direct primary obligations under the Data Protection Provisions to protect the personal data, give effect to access and correction requests, and include these overseas data repositories in its data retention policy.

16.4.4. *Rationale*: The Transfer Limitation Obligation is a manifestation of the Accountability Obligation. When an organisation discloses personal data to another organisation, and both are in Singapore, the receiving organisation is subject to the PDPA and has to protect the personal data that it receives. Likewise, when an organisation discloses personal data to its data intermediary, and both are in Singapore, the data intermediary is subject to the Protection, Retention Limitation and Data Breach Notification Obligations for the personal data that it thereby receives. However, when an organisation transfers personal data to another organisation that is outside Singapore (for example, a data intermediary or another company in the same group), the recipient organisation is not subject to

the PDPA. The Accountability Obligation requires that the transferring organisation takes steps to ensure that the recipient organisation will continue to protect the personal data that it has received to a standard that is comparable to that established in PDPA.

16.4.5. Conditions for transfer of personal data overseas

16.4.5.1. HReasily may transfer personal data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA.

16.4.5.2. **Legally enforceable obligations may be imposed in two ways.**

16.4.5.3. **First**, it may be imposed on the recipient organisation under:

a) any law;

b) any contract that imposes a standard of protection that is comparable to that under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract;

c) any binding corporate rules that require every recipient of the transferred personal data to provide a standard of protection for the transferred personal data that is comparable to that of the PDPA, and which specify

(i) the recipients of the transferred personal data to which the binding corporate rules apply;

(ii) the countries and territories to which the personal data may be transferred under the binding corporate rules; and

(iii) the rights and obligations provided by the binding corporate rules; or

d) any other legally binding instrument.

16.4.5.4. **Second**, if the recipient organisation holds a "specified certification" that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient organisation is taken to be bound by such legally enforceable obligations.

16.4.5.5. Under the Personal Data Protection Regulations 2021, "specified certification" refers to certifications under the Asia Pacific Economic Cooperation Cross Border Privacy Rules ("APEC CBPR") System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors ("APEC PRP") System.

16.4.5.6. **The recipient is taken to satisfy the requirements under the Transfer Limitation Obligation if:**

a) it is receiving the personal data as an organisation and it holds a valid APEC CBPR certification; or

b) it is receiving the personal data as a data intermediary and it holds either a valid APEC PRP or CBPR certification, or both.

16.4.5.7. PDPA encourages the reliance on the above legally enforceable obligations especially when they have an ongoing relationship with the recipient organisation because these provide better accountability.

16.4.5.8. **However, if the organisation is unable to rely on any of the above, PDPA can rely on the following circumstances:**

a) the individual whose personal data is to be transferred gives his consent to the transfer of his personal data, after he has been informed about how his personal data will be protected in the destination country;

b) the individual is deemed to have consented to the disclosure by the transferring organisation of the individual's personal data where the transfer is reasonably necessary for the conclusion or performance of a contract between the organisation and the individual, including the transfer to a third party organisation);

c) the transfer is necessary for a use or disclosure that is in the vital interests of individuals or in the national interest, and the transferring organisation has taken reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose;

d) the personal data is data in transit; or

e) the personal data is publicly available in Singapore.

16.4.6. Data in transit

16.4.6.1. Data in transit refers to personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed or used by, or disclosed to, any organisation (other than the transferring organisation or an employee of the transferring organisation acting in the course of his employment with the transferring organisation) while the personal data is in Singapore, except for the purpose of such transportation.

An example of data in transit would be data from overseas passing through servers within Singapore enroute to its destination overseas.

16.4.7. Overseas transfer of personal data to a data intermediary

16.4.7.1. Where HReasily engages a data intermediary to process personal data on its behalf and for its purposes, the organisation is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data.

16.4.7.2. This is regardless of whether the personal data is transferred by the organisation to an overseas data intermediary or transferred overseas by the data intermediary in Singapore as part of its processing on behalf and for the purposes of the organisation.

16.4.7.3. The Transfer Limitation Obligation requires that an organisation ensures that personal data transferred overseas is protected to a standard comparable with the Data Protection Provisions.

16.4.7.4. HReasily must undertake appropriate due diligence and obtain assurances when engaging a data intermediary to ensure that it is capable of doing so.

16.4.7.5. In undertaking due diligence, transferring organisations may rely on data intermediaries' extant protection policies and practices, including their assurances of compliance with relevant industry standards or certification.

16.5. Deemed Consent

16.5.1. Sections 15 and 15A of the PDPA provide for different forms of deemed consent, namely (a) deemed consent by conduct; (b) deemed consent by contractual necessity; and (c) deemed consent by notification.

16.5.2. Deemed consent by conduct

16.5.2.1. Deemed consent by conduct applies to situations where the individual voluntarily provides his personal data to the organisation. The purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances.

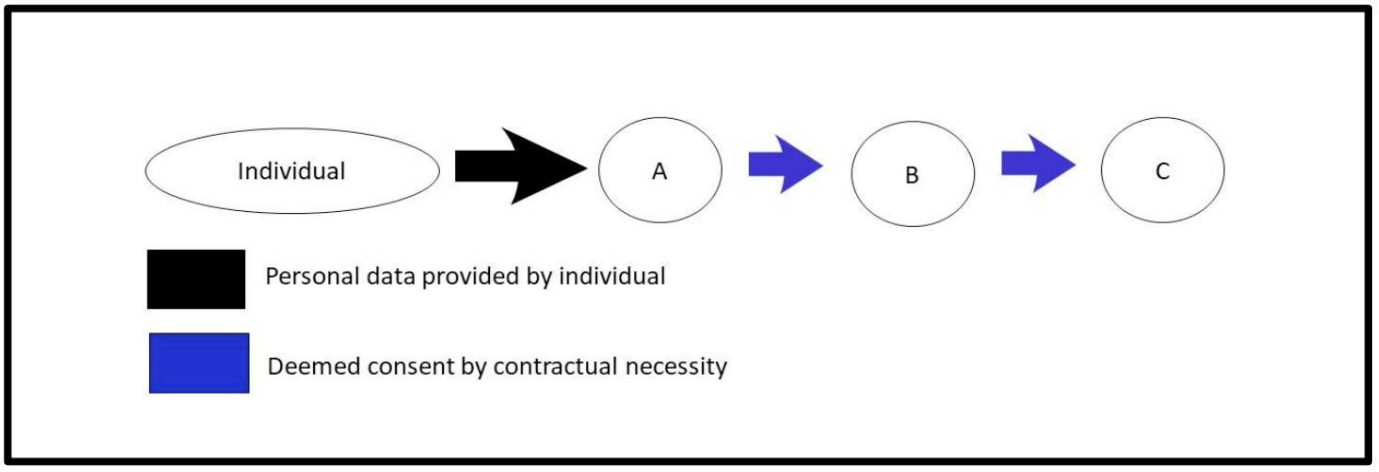
For example, providing personal data (resume) to respond to a job opening.

16.5.3. Deemed consent by contractual necessity

16.5.3.1. The second situation in which consent may be deemed is where an individual provides his personal data to one organisation ("A") for the purpose of a transaction and it is reasonably necessary for A to disclose the personal data to another organisation ("B") for the necessary conclusion or performance of the transaction between the individual and A.

16.5.3.2. Deemed consent by contractual necessity under section 15(3) extends to disclosure by B to another downstream organisation ("C") where the disclosure (and collection) is reasonably necessary to fulfil the contract between the individual and A.

16.5.3.3. To be clear, deemed consent by contractual necessity allows further use or disclosure of personal data by C and other organisations downstream (refer to Diagram 1 below) where the use or disclosure is reasonably necessary to conclude or perform the contract between the individual and A.



For example, Sarah is deemed to consent to a spa collecting, using or disclosing her credit card details to process the payment for her facial. In the course of processing the payment, her credit card details are transmitted to the spa's bank which handles the payment.

Since Sarah is deemed to consent to the disclosure of her credit card details by the spa to its bank, deemed consent by contractual necessity would apply to all other parties involved in the payment processing chain who collects or uses Sarah's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the contract between Sarah and the spa.

These parties include, for example, Sarah's bank, the spa's bank, the banks' processors and the credit card scheme's payment system providers.

16.5.4. Deemed consent by notification

16.5.4.1. Section 15A of the PDPA provides that an individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose that he had been notified of, and he has not taken any action to opt out of the collection, use or disclosure of his personal data.

16.5.4.2. This can be relied when the organisation wishes to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had originally collected the personal data for, and it is unable to rely on any of the exceptions to consent (e.g. business improvement, research) for the intended secondary use.

16.5.4.3. This is subject to the organisation assessing and determining that the following conditions are met, taking into consideration the types of personal data involved and the method of collection, use or disclosure of the personal data in the manner set out below:

a. **Conduct an assessment to eliminate or mitigate adverse effects.**

16.5.4.3.a.1. Section 15A(4)(a) of the PDPA provides that an organisation must, before collecting, using or disclosing any personal data about an individual, conduct an assessment to determine that the proposed collection, use or disclosure of personal data is not likely to have an adverse effect on the individual.

To conduct the assessment, follow the steps here: Assessment Checklists

16.5.4.3.a.2. This assessment should be recorded and a copy shall be retained for documentation throughout the period that the organisation collects, uses or discloses personal data based on deemed consent by notification.

16.5.4.3.a.3. When requested by the regulatory body, the organisation must provide its assessment for collecting, using or disclosing personal data based on deemed consent by notification.

16.5.4.3.a.4. The organisation is not required to provide its assessment to individuals who request for it as it may contain commercially sensitive information.

16.5.4.3.a.5. **Where it is assessed that there are likely residual adverse effects to the individual after implementing the measures, the organisation will not be able to rely on deemed consent by notification to collect, use or disclose personal data for the purpose.**

b. **Organisation must take reasonable steps to ensure that notification provided to individuals is adequate:** Section 15A(4)(b) of the PDPA provides that an organisation must take reasonable steps to bring the following matters to the attention of the individual:

(i) the organisation's intention to collect, use or disclose the personal data;

(ii) the purpose of such collection, use or disclosure; and

(iii) a reasonable period within which, and a reasonable manner by which, an individual can opt out of the collection, use or disclosure of his personal data for this purpose.

16.5.4.3.b.1. The regulatory body does not prescribe the method by which the individual should be notified, but the organisation must ensure the notification is adequate and effective in making the individual aware of the proposed collection, use or disclosure of his personal data.

c. **Organisation must provide a reasonable opt-out period.**

16.5.4.3.c.1. The organisation must provide a reasonable period for the individual to opt out before it proceeds to collect, use or disclose the personal data.

16.5.4.3.c.2. Consent for the collection, use or disclosure of personal data is deemed to be given only after the opt-out period has lapsed.

16.5.4.3.c.3. Any collection, use or disclosure of personal data for the purposes that have been notified should commence only after the expiry of the opt-out period.

16.5.4.3.c.4. **Some considerations for determining the reasonableness of the opt- out period include:**

(i) The nature and frequency of interaction with the individual. For instance, where an organisation sends push notifications through a mobile application used by individuals to track and update monthly medical check-up information, the opt-out period should not be shorter than one month.

(ii) The communications and opt-out channels used. Direct communications channels, particularly those that have a track record of being effective in reaching the intended customer base, may justify a shorter opt-out period than mass communications channels. Opt-out methods that are easily accessible and easy to use may also justify a shorter opt-out period (e.g. providing for opt-out via email or hyperlink).

16.5.5. Withdrawal of consent after opt-out period

16.5.5.1. After the opt-out period has lapsed and the individual no longer wishes to consent to the purpose, the individual can withdraw his consent for the collection, use or disclosure of personal data.

16.5.6. Consent for sending of directing marketing messages

16.5.6.1. Deemed consent by notification cannot be relied on for direct marketing messages.

16.5.6.2. Organisations should obtain express consent for the purpose of sending direct marketing messages to individuals.

16.5.6.3. Such consent should be obtained through the **opt-in method** (e.g. requiring action to check an unchecked box in order to give consent); the regulatory body does not consider the opt-out method (e.g. providing a pre-checked box and requiring action to opt-out) as appropriate for obtaining consent for the receipt of direct marketing messages.

16.5.6.4. **Consent obtained using the opt-out method will not constitute clear and unambiguous consent under the Do Not Call Provisions for sending a specified message to a Singapore telephone number registered on the Do Not Call Registry.**

16.6. Consent Withdrawal Policy

16.6.1. Withdrawal of consent

16.6.1.1. Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation.

16.6.1.2. **The following requirements must be complied with:**

a. the individual must give reasonable notice of the withdrawal to the organisation (section 16(1));
b. on receipt of the notice, the organisation must inform the individual of the likely consequences of withdrawing consent (section 16(2));
c. an organisation must not prohibit an individual from withdrawing consent, although this does not affect any legal consequences arising from such withdrawal (section 16(3)); and

d. upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law (section 16(4)).

16.6.1.3. HReasily must allow an individual who has previously given (or is deemed to have given) his consent to the organisation for collection, use or disclosure of his personal data for a purpose to withdraw such consent by giving reasonable notice.

As a general rule of thumb, the regulatory body would consider a withdrawal notice of at least ten (10) business days from the day the organisation receives the withdrawal notice, to be reasonable notice. Should an organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame by which the withdrawal of consent will take effect.

16.6.2. Consent withdrawal policy

16.6.2.1. In order to enable and facilitate withdrawal, HReasily should make an appropriate consent withdrawal policy that is clear and easily accessible to the individuals concerned.

16.6.2.2. **This withdrawal policy should:**

a. advise the individuals on the form and manner to submit a notice to withdraw their consent for specific purposes;

b. indicate the person to whom, or the means by which, the notice to withdraw consent should be submitted; and

c. distinguish between purposes necessary and optional to the provision of the products/services (that may include the service of the existing business relationship).

16.6.2.3. **Individuals must be allowed to withdraw consent for optional purposes without concurrently withdrawing consent for the necessary purposes.**

16.6.2.4. The organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual himself.

For example, if an organisation requires certain personal data from an individual in order to fulfil a contract with the individual to provide products or services, it may not stipulate as a term of the contract that the

individual cannot withdraw consent to the collection, use or disclosure of the individual's personal data for the purposes of the contract.

If the individual subsequently withdraws consent to his personal data in a manner which makes it impossible for the contract to be fulfilled, any legal consequences arising out of such withdrawal would not be affected.

16.6.2.5. If an individual has withdrawn his earlier consent to the collection, use or disclosure of his personal data by the organisation, but subsequently provides fresh consent to the organisation, the organisation may collect, use or disclose his personal data within the scope of the fresh consent that he subsequently provided.

16.6.3. Effect of withdrawal of notice

16.6.3.1. In determining the effect of any notice to withdraw consent, the regulatory body will consider all relevant facts of the situation.

16.6.3.2. **This could include but is not limited to matters like:**

a. the actual content of the notice of withdrawal;
b. whether the intent to withdraw consent was clearly expressed; and
c. the channel through which the notice was sent.

16.6.3.3. In cases where an organisation provides a facility for individuals to withdraw consent (e.g. by clicking on an "unsubscribe" link within an email), the organisation should clearly indicate the scope of such withdrawal.

16.6.3.4. **As best practice, the organisation may inform individuals of how they may withdraw consent for matters outside the scope of such withdrawal.**

16.6.3.5. In facilitating any notice to withdraw consent, an organisation should act reasonably and in good faith.

For example:

If you wish to stop receiving marketing messages from ABC via e-mail, please click on the link 'unsubscribe'. If you wish to stop receiving marketing messages from ABC via other channels, please send us an e-mail at dpo@abc.org.

16.6.4. Actions when receiving a notice of withdrawal

16.6.4.1. Once an organisation has received from an individual a notice to withdraw consent, HReasily should inform the individual concerned of the likely

consequences of withdrawing his consent, even if these consequences are set out somewhere else, e.g. in the service contract between the organisation and the individual.

16.6.4.2. Consequences for withdrawal of consent could simply be that the organisation would cease to collect, use or disclose the individual's personal data for the purpose specified by the individuals. In other cases, the organisation may not be able to continue providing services to the individual or there may be legal consequences.

16.6.4.3. With regard to personal data that is already in an organisation's possession, **withdrawal of consent would only apply to an organisation's continued use or future disclosure of the personal data concerned.**

16.6.4.4. Upon receipt of a notice of withdrawal of consent, the organisation must cease to collect, use or disclose the individual's personal data, and inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the various purposes.

16.6.4.5. Apart from its data intermediaries and agents, an organisation is not required to inform other organisations to which it has disclosed an individual's personal data of the individual's withdrawal of consent.

16.6.4.6. This does not affect the organisation's obligation to provide, upon request, access to the individual's personal data in its possession or control and information to the individual about the ways in which his personal data may have been disclosed.

16.6.4.7. Hence the individual may find out which other organisations his personal data may have been disclosed to and give notice to withdraw consent to those other organisations directly.

16.6.4.8. Although an individual may withdraw consent for the collection, use, or disclosure of his personal data, the organisation is not required to delete or destroy the individual's personal data upon request.

16.6.4.9. HReasily may retain personal data in documents and records in accordance with the Data Retention policy.

16.7. Exceptions to the Consent Obligation

16.7.1. Legitimate interests exception

16.7.1.1. "Legitimate interests" generally refer to any lawful interests of an organisation or other person (including other organisations).

16.7.1.2. To rely on this general exception, the organisation should assess the adverse effects and ensure the legitimate interests outweigh any adverse effect.

16.7.1.3. As the legitimate interests exception allows the collection, use or disclosure of personal data without consent for a wide range of circumstances and purposes, the organisation seeking to rely on this exception must comply with additional safeguards to ensure that the interests of individuals are protected.

16.7.1.4. **HReasily must assess that they satisfy the following requirements before relying on the legitimate interests exception:**

a. **Identify and articulate the legitimate interests.** Organisations must identify and be able to clearly articulate the situation or purpose that qualifies as a legitimate interest.

b. **Conduct an assessment.** HReasily must conduct an assessment before collecting, using or disclosing personal data (as the case may be) to:

(i) identify any adverse effect that the proposed collection, use or disclosure is likely to have on the individual; and

(ii) identify and implement reasonable measures to eliminate, reduce the likelihood of or mitigate the adverse effect on the individual.

16.7.1.4.b.1. Where it is assessed that there is likely residual adverse effect to the individual after implementing the measures, organisations are required to conduct a balancing test as part of the assessment to determine that the legitimate interests of the organisation or other person (including other organisations) outweigh any likely residual adverse effect to the individual.

16.7.1.4.b.2. **The organisation may rely on the legitimate interests exception if the legitimate interests outweigh any likely residual adverse effect to the individual.**

HReasily's assessment criteria is stipulated here:Assessment Checklists

c. Disclose reliance on the legitimate interests exception.

16.7.1.4.c.1. When relying on the legitimate interests exception to collect, use or disclose personal data without consent, the organisation must take reasonable steps to provide the individual with reasonable access to information that they are relying on the exception.

16.7.1.4.c.2. This may be through any means that is reasonably effective (e.g. disclosure as part of the organisation's privacy policy).

PDPA does not allow organisations to rely on the legitimate interests exception to send direct marketing messages.

In general, organisations must obtain express consent to send direct marketing messages to individuals.

In addition, where direct marketing messages are sent to Singapore telephone numbers via voice call, text or fax, the organisation must comply with the Do Not Call Provisions of the PDPA

16.7.1.5. Examples of legitimate interests

a. purposes of detecting or preventing illegal activities (e.g. fraud, money laundering) or threats to physical safety and security, IT and network security;

b. preventing misuse of services; and carrying out other necessary corporate due diligence.

c. Subjecting such purposes to consent is not viable as individuals may choose not to give consent or to withdraw any consent earlier given (e.g. individuals who intend to or who had engaged in illegal activities), impeding the organisations' ability to carry out such functions.

16.7.2. Business improvement exception

16.7.2.1. PDPA allows the organisation to **use**, without consent, personal data that was collected where the use of the personal data falls within the scope of any of the following business improvement purposes:

a. Improving, enhancing or developing new goods or services;
b. Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;
c. Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or
d. Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

16.7.2.2. **In order to rely on the business improvement exception, the organisation must ensure the following:**

a. The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form; and
b. The organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

16.7.2.3. The business improvement exception also applies to the **sharing of personal data (i.e. collection and disclosure) between entities belonging to a group of companies, without consent,** for the following business improvement purposes:

a. Improving, enhancing or developing new goods or services;
b. Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;
c. Learning or understanding behaviour and preferences of existing or prospective customers (including groups of individuals segmented by profile); or
d. Identifying goods or services that may be suitable for existing or prospective customers (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

16.7.2.4. **Organisations relying on the business improvement exception to share personal data within the group will need to ensure the following:**

a. The business improvement purpose cannot reasonably be achieved without sharing the personal data in an individually identifiable form;
b. The organisations' sharing of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances; and
c. The organisations involved in the sharing are **bound by any contract or other agreement or binding corporate rules** requiring the recipient(s) of personal data to implement and maintain appropriate safeguards for the personal data.

Business insights relating to individuals will be considered personal data if an individual can be identified from that data, including other information that the organisation has or is likely to have access (e.g. insights and predictions generated about a specific individual).

The regulatory body recognises that it may be necessary for organisations to share data regarding customer behaviour and preferences to improve products as part of the feedback loop in product development.

For this case, the organisation may rely on the business improvement exception as the sharing of personal data is relevant to the eventual aim of improving, enhancing or developing new goods or services.

The organisation cannot rely on the business improvement exception to send direct marketing messages.

Organisations must obtain express consent to send direct marketing messages to individuals.

In addition, where direct marketing messages are sent to Singapore telephone numbers via voice call, text or fax, the organisation must comply with the Do Not Call Provisions of the PDPA

16.7.3. Sending of direct marketing messages and preparatory activities to marketing

16.7.3.1. To be clear, the organisation cannot rely on the exceptions for legitimate interests or business improvement for the purpose of sending direct marketing messages.

16.7.3.2. However, the organisation may rely on the business improvement exception to use existing customers' personal data for **data analytics and market research** to derive insights and understand their existing customers prior to their business marketing activities.

16.7.3.3. The regulatory body considers these to be **preparatory activities for marketing purposes** and are to be distinguished from the sending of direct marketing messages to individuals.

16.7.4. Research exception for the use and disclosure of personal data without consent

16.7.4.1. The research exception is intended to enable the organisation to conduct broader research and development that may not have any immediate application to their products, services, business operations or market.

16.7.4.2. Commercial laboratories that carry out research for the development of science, institutes of higher learning that conduct research into the arts and social sciences, and organisations that carry out market research are examples of organisations that can continue to rely on the research exception.

16.7.4.3. The research exception provides that organisations may **use** personal data for a research purpose, including **historical and statistical research**, subject to the following conditions:

a. The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

b. There is a clear public benefit to using the personal data for the research purpose;

c. The results of the research will not be used to make any decision that affects the individual; and

d. In the event the results of the research are published, the organisation must publish the results in the form that does not identify the individual.

16.7.4.4. The organisation may rely on the research exception to **disclose** personal data for a research purpose, including historical and statistical research. All the conditions for use of personal data for a research purpose are applicable together with the following **additional condition**:

a. It is impracticable for the organisation to seek the consent of the individual for the disclosure.

See Advisory Guidelines on Key Concepts in the PDPA 1 Feb 2021 §12.82 in assessing whether it is "impracticable" to seek consent.

16.7.5. Publicly available data

16.7.5.1. Publicly available personal data refers to personal data (about an individual) that is generally available to the public, including personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

16.7.5.2. Personal data is generally available to the public if any member of the public could obtain or access the data with few or no restrictions. In some situations, the existence of restrictions may not prevent the data from being publicly available.

For example, if personal data is disclosed to a closed online group but membership in the group is relatively open and members of the public could join with minimal effort, then the disclosure may amount to making the data publicly available.

Conversely, if personal data is disclosed to a close circle of the individual's family and friends or it is inadvertently disclosed to a single member of the public who is not personally known to the individual concerned, the disclosures may not make the personal data publicly available.

16.7.5.3. The regulatory body recognises that personal data that is publicly available at one point in time may, for various reasons, no longer be publicly available after that time.

For example, users of social networking sites may change their privacy settings from time to time, which would have an impact on whether their personal data would be considered publicly available.

16.7.5.4. The regulatory body recognises that it would be excessively burdensome for the organisation intending to use or disclose publicly available personal data without consent to constantly verify that the data remains publicly available, especially in situations where the use or disclosure happens some time after the collection of the personal data.

16.7.5.5. Hence, the regulatory body takes the position that so long as the personal data in question was **publicly available at the point of collection**, the organisation will be able to **use and disclose** personal data without consent under the corresponding exceptions, notwithstanding that the personal data may no longer be publicly available at the point in time when it is used or disclosed.

16.7.5.6. Publicly available personal data also includes a category of personal data that is specifically included in the definition, that is, personal data observed in public. For this to apply, there are two requirements relating to how and where the personal data is observed:

a. the personal data must be observed by reasonably expected means; and
b. the personal data must be observed at a location or event at which the individual appears and that is open to the public.

17. Data Retention, Archiving and Destruction Policy

17.1. Purpose

The purpose of this Data Retention, Archiving and Destruction Policy is to ensure that the data collected, maintained and used by HR Easily Pte Ltd, including sensitive personal data, is adequately protected and maintained, and to ensure that data that is no longer needed by company is discarded at the proper time and in the proper manner.

17.2. Definitions

Anonymisation

The process of turning data into a form which does not identify individuals. It is a type of information sanitization whose intent is privacy protection.

HRE is considered to have ceased to retain personal data when it no longer has the means to associate the personal data with particular individuals – i.e. the personal data has been anonymised.

Archiving

The process of moving data that is no longer actively used to a separate storage device or location for retention.

Asset Owner

The functional or business head who is responsible for the Data Asset (or within whose function or business line the asset resides or is used).

Data Asset

Any item or entity that comprises data. For example, databases are data asset that comprise records. A data asset may be a system or application output file, database, document, or webpage. A data asset may also include a means to access data from an application.

Destruction

Defined as physical or technical destruction sufficient to render the information contained in the document irretrievable by ordinary commercially available means.

Document

As used in this Policy, is any medium which holds Information used to support an effective and efficient organizational operation. Examples of Documents include:

(a) Policies

(b) Quality Criteria

(c) Procedures

(d) Tools and Templates

Financial Records

Pieces or sets of information related to the financial health of a business. The pieces of data are used by internal management to analyze business performance and determine whether tactics and strategies must be altered

Personal Data (also "*Personally Identifiable Information*")

Any information relating to an identified or identifiable natural person (the "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Record

As used in this Policy, is any medium which holds information or evidence about a past event. Examples of Records include:

(a) Case records

(b) Reports

(c) Minutes

(d) Video and audio recordings

(e) Data generated by physical access control systems

Human Resources Record

Any information about an employee's eligibility for employment, promotion, compensation, transfer, termination, disciplinary or other adverse action (such as, evaluations or reports related to the employee's character, credit, and work habits)

The contents of this record may be maintained in paper or electronic format and the following are examples:

(a) Pre-employment records (employment application, resume, offer/acceptance letter);

(b) Hiring records (confidentiality agreement, conflict of interest questionnaire, arbitration agreement, sign-on bonus agreement);

(c) Attendance records (attendance management reports, leave notifications);

(d) Compensation statements (salary increases, bonuses, long-term incentives);

(e) Disciplinary process documents (performance, behaviour, warnings);

(f) Flexible work agreements and related information;

(g) Performance appraisals;

(h) Development plans;

(i) Training, development, and education courses (certificates of completion);

(j) Notes of commendation or discipline;

(k) Termination documents (resignation letter);

(l) Exit interviews

Retention

The continued processing of data, after the initial "active use" has achieved the purpose for which the data was originally collected.

Data Retention is usually required to meet applicable legal or contractual obligations or meet business objectives. Retention Periods are determined accordingly. For Personal Data they must be no longer than necessary to protect the rights and freedoms of individual data subjects in accordance with applicable Data Protection regulations.

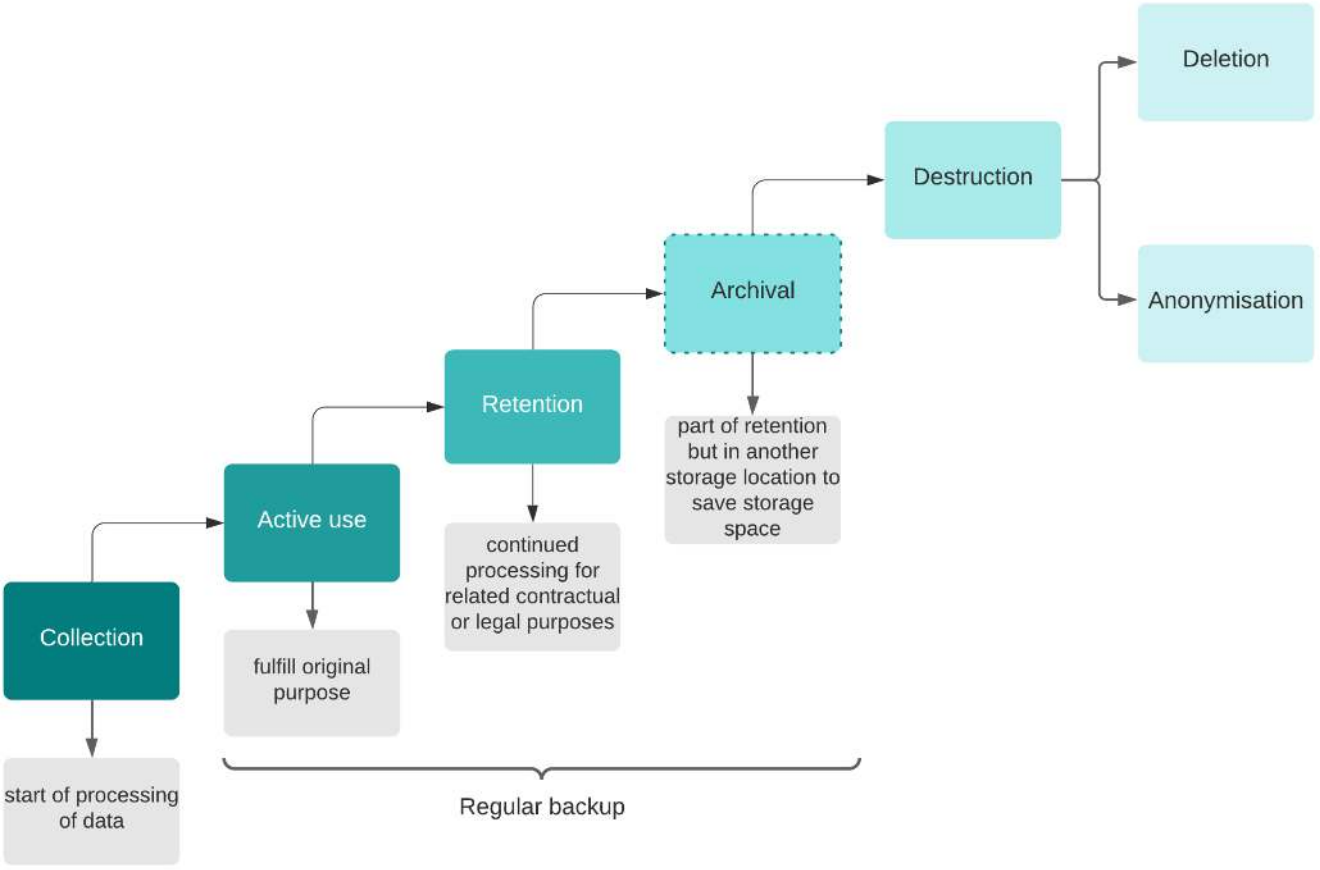
In some cases, retention may be in the form of "Archival", to preserve storage space or bandwidth on the system or container originally employed for Active Use processing.

Throughout the data processing, for Information Security and Disaster Recovery and Business Continuity purposes, regular back-ups or copies may be created of the data. Retention periods of such back-ups should be only as long as required to fulfil this purpose.

The retention periods are generally determined by evaluating:

- Applicable regulatory, statutory, legal, or general country compliance requirements
- Determining electronic data components collected, their purpose, and applying the appropriate retention procedure to each class of data asset

- Identifying other internal or external entities that collect, store, archive, or use HRE information and records



The Data Processing Lifecycle

17.3. Data Retention and Archiving

It is impossible to designate a retention period for each and every type of data that may exist or come to exist. However, this policy sets forth Retention Periods for certain common types of Data in the table below. If certain data does not fall within a class for which there is a designated retention period in this policy, HRE will consult with legal counsel to determine the proper classification of the data or to establish a retention period for the data in question.

To the extent data is subject to more than one retention period, the data will be retained for the longer of the specified time frames in order to comply with this policy.

For the purposes of enforcing retention in accordance with this policy, each function is responsible for the records and documents it creates, uses, stores, processes and destroys.

Data logs and backup are retained for as long as there is business, legitimate and regulatory reasons to do so

- To allow for analysis and investigations should the need arises, our standard retention period is a minimum of one (1) year and maximum of seven (7) years
- In cases where individual country laws exceed seven (7) years, we will retain data for as long as legally mandated

The company's standard retention periods for categories of data are:

Categories of Data	Retention period	Notes
Resume or CV as collected by HR and third-party vendors	Standard retention period	Personal data protection ordinances or other legal or regulatory requirements apply
HR Records	Standard retention period	**Singapore Employment Act** - For current employees, latest 2 yrs - For former employees, last 2 yrs, to be kept for 1 yr after the employee leaves employment
Accounting and financial records (e.g. employee or company payroll records, billing information) Accounting records are key sources of information and evidence used to prepare, verify and/or audit the financial statements. They also include documentation to prove asset ownership for creation of liabilities and proof of monetary and non monetary transactions.	Eight (8) years or more based on applicable regulations. Standard practice is to add one year based on the country's statute of limitation (e.g. 7 years + 1)	**Malaysia: Income Tax Act of 1967** has a 7yr retention period, "All taxable persons are required to keep sufficient accounts affecting their liability for income tax for 7 years." **Indonesia / Philippines Accounting law**: Annual balance sheets, accounts, daily transaction journals, and other accounting records must be retained for 10 years following the year to which they pertain. Tax law: Accounting books and records as well as other business documents that support the calculation and payment of taxes must be retained for 10 years. **Hong Kong Accounting law and Tax law**: minimum of 7 years
Company financial statements, permanent financial audits	Permanent	Tax return, results of an audit by a tax authority, general ledgers, and financial statements should normally be kept indefinitely.

Procurement and Contracts (Expired) Records of evidence of all actions taken to award contracts, and of the monitoring and oversight of contract implementation. These are the basis for internal and external audits, and are needed to determine compliance with the legal or regulatory frameworks.	Seven (7) years or based on applicable regulations	**Indonesia Contract law**: The general statute of limitations for civil litigation related to obligations is 30 years unless a different period is specified by law. The statute of limitations to nullify a contract for reasons of duress, error, or fraud is 5 years. **Philippines**: 10 years from the date a written contract was breached, and 6 years from the date that a non-written contract was breached. **Hong Kong**: 6 years
Collected personal data from events, webinars, etc • Marketing Sign-up: Hubspot, Discord • Marketing Newsletter Sign-up: Hubspot, Wordpress backend • Marketing Enquiries form: Hubspot, Wordpress backend • Marketing: Facebook, EventBrite	Standard retention period	Personal data protection ordinances or other legal or regulatory requirements apply
Collected personal information from Sales processes (e.g. Calenly information for bookings)	Standard retention period	Personal data protection ordinances or other legal or regulatory requirements apply
Academy Data Flow (Customer Experience) after termination of subscription or withdrawal of consent	Standard retention period	Personal data protection ordinances or other legal or regulatory requirements apply
Customer company and employee data after termination of subscription or withdrawal of consent (includes personal and sensitive data)	Standard retention period or based on applicable regulations or based on client requirements* *only when there are contractual agreements between parties	Personal data protection ordinances or other legal or regulatory requirements apply

Penetration testing reports, audit logs, IT-related audits	Standard retention period or based on applicable regulations	CIS Controls require that we retain audit logs for at least 90 days before archiving it.
Other documents and records	Standard retention period or based on applicable regulations	Legal or regulatory requirements apply

17.4. Retention and Archiving exceptions

An archiving period more or less than the period stated in the summary table may be granted with an exception. These exceptions should have legal or regulatory basis such as client requests, business requirement, on-going litigation, investigation or other legal proceedings until any dispute is fully resolved and no longer open to appeal.

If an employee is aware of any anticipated or existing litigation, the employee should notify the Data Protection Officer, so they can suspend any deletion or anonymisation of personal data.

A retention period lesser than the period stated in this policy should relate to records with a limited business purpose such as email, travel itineraries, advisories, or to comply with client or industry requirements.

17.5. Archiving Policy

HRE can process personal data for archiving purposes beyond the stated retention period if doing so is in the **public interest**, or for **historical**, **scientific** or **statistical purposes**.

We ensure that archiving does not contravene the rights and freedoms of data subjects and that appropriate technical and organisational safeguards are in place, such as data minimisation, pseudonymisation or encryption.

17.6. Data Destruction

17.6.1. Regular Review

All Data, whether held electronically, on individual employees' devices or on paper, should be reviewed on a regular basis to decide whether to destroy or delete any Data in accordance with the designated retention period.

Responsibility for the destruction of data included in the Data Asset Inventory falls to each Asset owner.

17.6.2. Safe Destruction and Disposal

Personal Data or confidential or restricted information must be disposed of as confidential waste and be subject to secure electronic deletion or anonymisation.

Some expired or superseded contracts may only warrant in-house shredding.

Paper Documents shall be shredded using secure, locked consoles designated in each office from which waste shall be periodically picked up by security screened personnel for disposal.

The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that HRE subcontracts for this purpose.

All external service providers must be thoroughly vetted and reviewed to ensure their full compliance with data protection requirements, and all data disposal is subject to applicable provisions under relevant data protection laws and HRE Information Security Policy.