heardat
Success Simplified

Access Control and Security Policy

Section: Access, Security & Restrictions

Prepared by:	Barend Botha, Kieara Smit, Charl Bezuidenhout
Approved by:	C.I. Bezuidenhout
Revision date:	5 May 2020
Effective date:	7 May 2020

Statement of Policy and Procedures relating to "Heardat Access and Security"

Manual	Information Technology	**SPP No**	HDAS 2.0
Section	Access Security & Restrictions	**Issued**	7 May 2020
Subject	Access & Security Policy	**Effective**	7 May 2020
Issue to	Employees, clients & users, external contractors	**Pages**	1-3
Issued by	Charl Bezuidenhout	**Replaces**	HDAS 1.0 (October 2017)

1. Policy Statement

1.1. Protecting access to Heardat system portals, applications and coding is critical to maintain the integrity of Heardat and its system portals and prevent unauthorized access to such information.

1.2. Access to Heardat system portals must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

2. Purpose

2.1 The objective of this policy is to ensure the Company has adequate controls to restrict access to system portals, accounts, information and data.

2.2 Restrict and protect access & clearance levels to Heardat systems and information for employees, users, clients and their employees.

3. Scope

3.1. All Heardat offices, workspaces and computer hardware.

3.2. All Heardat employees, consultants, contractors, agents, and authorized users accessing Heardat system portals and applications.

3.3. All IT systems or applications managed by Heardat that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

4. Responsibility

4.1 All employees of Heardat, contractors, third parties and/or affiliated personnel whom has granted permission and/or access to system portals hosted by Heardat.

5. Definitions

5.1 **"Critical data"** is that data which is needed to continue the operation of a business.

5.2 **"Data backup"** means making a copy of data such that the copy may be used easily to recreate the original data organized in its original format.

5.3 **"Data medium"** means a physical object on which data may be stored (e.g., magnetic tape, tape cartridge, optical disk [CD-ROM, DVD], disk cartridge [ZIP, IOMEGA, 3M SuperDisk], or removable hard drive). Other historical data media not typically used today include punch cards and paper tape.

5.4 **"Offsite"** means a physical location other than where data is being processed. Its location must be far enough removed so that data stored offsite is not subject to the same physical risk from foreseen disasters. Note that if the objective is to protect against data loss in the event of a building fire or other disaster that restricts access to the building, a location in the same or adjacent building is not suitable as an offsite storage location.

6. Procedures

6.1 The backup copies must be on a storage device physically separate from the original. For example, if the data to be backed up is on a hard drive, the backup copy must be on a different hard drive and on the minimum of 2 cloud servers not affiliated with each other.

6.2 The backup data must be on a medium and in a format that can be easily used to recreate the data that has been damaged; however, it need not be identical to the original medium provided that the data may be restored to the original medium. For example, if the original data is on a hard drive, the backup may be on a removable disk, tape or optical medium from which the data may be copied back to a replacement hard drive in its original format. If the original data is organized in a specific database type, the copy must have enough information to recreate the database. However, the main source of data storage and backup remains within the cloud servers.

6.3 For offsite backups, the following must be maintained:

6.3.1 List of offsite locations where backup data may be easily located and retrieved.

6.3.2 List of procedures that create backup data and cause it to be shipped and stored at the backup site. In the case of more than one offsite location, each entry in the list also includes a reference to the corresponding offsite backup location.

6.3.3 All data of the Heardat Client remains the clients property. Heardat act as a tool to process data in the desired way.

6.3.4 No data may be altered or changed, added or deleted with out written concent from the client.

7. User Access Permissions

7.1 Company Manager: This is the highest level of clearance a user can have. This gives you access to the collective company's information, settings etc.

7.2 Branch Manager: This clearance level can access the specific branches' settings and patient data. The same permissions as the Company Manager 's permissions but only for the specific branch where the user is assigned to.

7.3 Users: View and work with all features, only in branches allocated to them. No access to settings.

7.4 Administrator: Only Heardat's support staff is assigned at this clearance level. The user has access to all settings and patient data. The user also as has access to certain and limited back end settings.

The End