	<b>GENERAL MANAGEMENT</b>	No. 000.5980.000	The 01 <sup>st</sup> draft was approved on: May 16, 2022
	<b>INSTITUTIONAL POLICY REDOME</b>	<b>PAGE 1 of 6</b>	This draft was approved on: May 16, 2022
			<b>DOCUMENT VERSION No.: 00</b>
	<b>IT POLICY</b>		

## 1. Purpose

Establishing a set of procedures and responsibilities seeking greater security and availability in the use of computer resources (equipment, systems, applications, software), to be practiced by all REDOME employees and service providers, ensuring the maintenance and continuity of the activity.

## 2. Definitions and Abbreviations

REDOME – Brazilian Registry of Volunteer Bone Marrow Donors;

IT – Information Technology;

Users – Employees and service providers authorized to access and use REDOME's software and/or equipment.

Encryption – A technique by which information can be transformed from its original form into an unreadable one, so that it can only be known to its recipient.


Systems and Applications – A set of programs, screens and functionalities developed internally or externally by other companies or acquired in the form of packages.

## 3. Coverage

This policy applies to employees and service providers who use or access REDOME's IT resources (equipment, application systems, software).

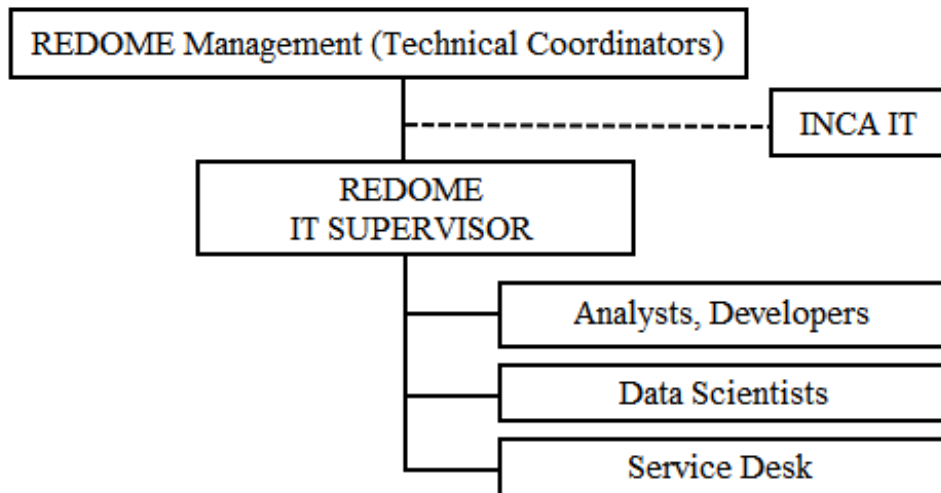
## 4. Reference documents

Document name	Description
Law No. 13,709, of August 14, 2018, called the General Personal Data Protection Law	General Law for the Protection of Personal Data.
<i>Topologia Inca.pdf</i>	INCA network topology.
<i>Processo Rotina de backup.pdf</i>	Database backup and restore routines.
<i>Processo Varredura de vulnerabilidades.pdf</i>	Vulnerability testing and scanning process.

	<b>GENERAL MANAGEMENT</b>	No. 000.5980.000	The 01 <sup>st</sup> draft was approved on: May 16, 2022
	<b>INSTITUTIONAL POLICY REDOME</b>	<b>PAGE 2 of 6</b>	This draft was approved on: May 16, 2022
			<b>DOCUMENT VERSION No.: 00</b>
	<b>IT POLICY</b>		

Advanced_Scan_DMZ_tk96cn.pdf	Evidence of vulnerability testing.
Most_important_Web_App_Tests_wnwkin.pdf	Evidence of vulnerability testing.
Web_App_DMZ_uoznvq.pdf	Evidence of vulnerability testing.
<i>Termo de Uso e Política de Privacidade.doc</i>	Describes the rules and guidelines for using the systems, as well as the rights and duties of REDOME related to the privacy of user data


## 5. Organizational Structure - INFORMATION TECHNOLOGY



## 6. Responsibilities

### 6.1. REDOME Employees in General

- a. Taking care of the IT resources under their responsibility, or to which they may have access;
- b. Protecting all information to which they have access, under their responsibility;
- c. Reporting any situation related to the use of IT resources, which may jeopardize the continuity of activities or processes.

	<b>GENERAL MANAGEMENT</b>	No. 000.5980.000	The 01 <sup>st</sup> draft was approved on: May 16, 2022
	<b>INSTITUTIONAL POLICY REDOME</b>	<b>PAGE 3 of 6</b>	This draft was approved on: May 16, 2022
			<b>DOCUMENT VERSION No.: 00</b>
	<b>IT POLICY</b>		

## 6.2. INFORMATION TECHNOLOGY department

- a. Ensuring the availability of IT resources so as not to generate delays or losses in any process, seeking the non-discontinuity of operations;
- b. Making efforts in search for solutions for interruptions, seeking to eliminate or minimize losses to operations, as much as possible;
- c. Monitoring and implementing the procedures proposed in this policy, ensuring its updating and protection regarding the inappropriate use of IT resources, changes in legislation and/or in the activity's requirements.


## 7. Procedures

### 7.1. Access control

- a. All access to the network, systems and applications must be carried out through user identification, individually, authenticated with a password;
- b. Passwords must be confidential, individual and non-transferable, and must not be disclosed under any circumstances;
- c. The access granted to users to systems and applications must strictly correspond to what is necessary for the execution of their activities, according to predefined profiles.
- d. In compliance with the General Law for the Protection of Personal Data (LGPD), every user of the systems and applications provided by REDOME must sign the Terms of Use and the Privacy Policy. This document describes the rules and guidelines for using the systems, as well as REDOME's rights and duties related to the privacy of user data.
- e. Accounts with administrative privileges to access databases and servers will only be granted to the IT team.

### 7.2. Data Encryption

- a. Systems that contain confidential information use cryptographic mechanisms to protect this information. This procedure mainly applies to electronic data transmissions to other registries;

	<b>GENERAL MANAGEMENT</b>	No. 000.5980.000	The 01 <sup>st</sup> draft was approved on: May 16, 2022
	<b>INSTITUTIONAL POLICY REDOME</b>	<b>PAGE 4 of 6</b>	This draft was approved on: May 16, 2022
			<b>DOCUMENT VERSION No.: 00</b>
	<b>IT POLICY</b>		

- b. Systems available online, through which confidential information travels, use the SSL protocol.

### **7.3. Electronic Auditing and Monitoring**

- a. The registration of recipients (patients) and donors are made electronically, through proprietary systems, and stored in a database located in INCA's Infrastructure department.
- b. Patient and donor records will remain in the database for an unlimited time. Their status may change, but any deletion will only be logical, not discarding the record.
- c. Donors over the age of 60 will automatically receive a “REMOVED” status through a routine performed daily.
- d. All systems developed by REDOME must contain audit records (logs).
- e. These records must be filed containing the date/time of occurrence, and identify the executing user.
- f. All logs must be protected, and only users with specific and restricted profiles can access and delete data.

### **7.4. Tests and Approval**


Every system developed or acquired by REDOME must be tested and approved before being put into production.

### **7.5. Documentation**

Every system developed or acquired by REDOME must have an administration manual, containing installation procedures, security procedures and version update procedures.

### **7.6. Security Architecture**


- a. Development, approval and production environments must be physically and logically isolated in order to:
  - I. Reduce the physical access of external people to the environments.
  - II. Reduce developer access to the production environment.
  - III. Ensure the quality of the security functions of the generated system.

	<b>GENERAL MANAGEMENT</b>	No. 000.5980.000	The 01 <sup>st</sup> draft was approved on: May 16, 2022
	<b>INSTITUTIONAL POLICY REDOME</b>	<b>PAGE 5 of 6</b>	This draft was approved on: May 16, 2022
			<b>DOCUMENT VERSION No.: 00</b>
	<b>IT POLICY</b>		

- b. Applications should only be moved from the development environment to homologation after successfully completing the removal of debugging information.
- c. Applications should be moved from the staging environment to production only after successful completion of all anticipated functional security and vulnerability testing.
- d. The architecture of the homologation environment must be as similar as possible to the production environment, in order to guarantee the quality of the tests and avoid the masking of failures.
- e. All infrastructure (servers, network, firewall, database) is provided and must be maintained by INCA's IT Infrastructure, including security procedures such as backup, network security and vulnerability testing.
- f. INCA's network topology is described in the document **“Inca Topology”**.
- g. Environment vulnerability tests are performed monthly, under the responsibility of INCA's IT Infrastructure. The scanning process is described in the document **“Vulnerability Scanning Process”**.
- h. The REDOME IT department must be called by users, via email or through a helpdesk system, whenever errors occur in the systems and applications installed; the error, screen or function that was being used must be described, including a print of the screen attached to it, if possible.

### **7.7. Backup and Restore**

- a. Critical data stored on laptop and workstation hard drives must be transferred to the appropriate location on the network as soon as possible, in order to ensure its updating and proper backup.
- b. When it is necessary to remove or change equipment, the IT department must proceed with the complete elimination of all stored information, preceded by a backup of critical data. This procedure must also be followed in cases of removal of equipment for maintenance and repairs.

	<b>GENERAL MANAGEMENT</b>	No. 000.5980.000	The 01 <sup>st</sup> draft was approved on: May 16, 2022
	<b>INSTITUTIONAL POLICY REDOME</b>	<b>PAGE 6 of 6</b>	This draft was approved on: May 16, 2022
			<b>DOCUMENT VERSION No.: 00</b>
	<b>IT POLICY</b>		

- c. Daily backups are made. The IT Infrastructure department of INCA is responsible for all backup and restore procedures. These procedures are described in the document “**Routine Backup Process**”.

### **7.8. Change Management**

- a. Changes or updates to the production environment must be previously reviewed and tested, in a homologating environment, for impacts on systems and applications, avoiding their unavailability, or failures that could compromise security.
- b. The approval of changes in the production environment must be carried out only after their homologation; based on the result of these procedures, it must also be formal and documented.
- c. The documentation related to systems and applications (example: administration and user manuals) must be reviewed and updated in case of changes in the production environment that affect any established procedure.

### **8. Complementary Documentation**

- Terms of Use and Privacy Policy - intended for users of REDOME systems
- Confidentiality and Data Security Policy - intended for donors registered in REDOME