PRIVACY AND SECURITY POLICY

DNS WOMEN INSTITUTE

DATA SECURITY POLICY

1- PURPOSE

DNS WOMEN has an obligation to restrict access to confidential and sensitive data to protect them against loss or compromise, avoiding adverse impacts to our customers, our own company and our employees.
DNS WOMEN guarantees holders access to their data as necessary for them to function effectively.
DNS WOMEN works to minimize events of theft and actions that damage data, although it is aware that it is not possible to guarantee that all risks will be eliminated.
DNS WOMEN seeks to increase user awareness and prevent accidental loss scenarios.
In this Policy the company describes the data breach prevention requirements.

2- SCOPE

This Data Security Policy is applicable to all data of the holder, general or sensitive personal data, according to the LGPD.
This Policy applies to all servers, databases and IT systems that handle this data, including any device that is regularly used for email, web access or other work-related tasks.
Every user, internal or external, who interacts with the company's IT services is also subject to this Policy.
o Are outside the scope of this Policy: Information classified as public is not subject to this Policy and other data may be excluded from the DNS WOMEN Policy based on specific business needs, such as to protect high cost or very complex data.

3- DEFINITIONS

For the purposes of understanding and easy understanding of this Policy, the following are the definitions and concepts that will be used throughout this document:
The. Data: part of the structure unable to generate intelligible but computable conclusions. Represents a non-described action, a quantity without specifying the object.
B. Personal data: all types of data that can lead to the identification of a person, directly or indirectly. Some types of personal data include (full name, RG, CPF, address, telephone, e-mail, IP address, date of birth, among others).
w. Sensitive data: Any information about a natural person related to racial, ethnic, creed, political opinion, union membership, health, sex, genetic and biometric data.
d. Anonymized data: operation performed with personal data in order to make them anonymous or make it difficult to identify the individual.
It is. Public data: data that is still public can be restricted by the individual.
f. ANPD - National Data Protection Authority: body of the direct federal public administration with duties related to regulation and inspection of compliance with the LGPD.
g. Holder: person to whom the personal data that are subject to treatment refer.
H. Controller: natural or legal person, who is responsible for decisions regarding the processing of personal data.
i. Operator: natural or legal person processing personal data on behalf of the controller.

j. Data officer: responsible before the ANPD and the holders indicated by the controller, in accordance with the LGPD.
k. Data processing: any operation carried out with personal data (including: access, storage, archiving, classification, collection, communication, control, dissemination, distribution, elimination, extraction, modification, processing, production, reception, reproduction, transfer, transmission and use).
l. Customer: natural or legal person who hires the company's services.
m. Collaborator: natural person who is part of the DNS WOMEN staff.
n. Partner/supplier: individual or legal entity that provides services to DNS WOMEN within the scope of its activities.
O. Technological resources: all physical and digital resources used to create, store, handle, transport, share and dispose of information. Among the types of resources we can highlight: desktop or laptop computers, smartphones, tablets, pen drives, external disks, media, printers, scanner, cloud services, among others.
P. Mobile Device: Any electronic device with mobility assignments.
q. Anonymization: use of reasonable technical means available at the time of processing, through which data loses the possibility of direct or indirect association with an individual.
r. LGPD - General Personal Data Protection Law: Law No. 13.709/2018 that "provides for the processing of personal data, including in digital media, by individuals or legal entities governed by public or private law, with the aim of protecting fundamental rights of freedom and privacy.
s. Encryption: Conversion of data from a readable format into an encoded format. Encrypted data can only be read or processed after it has been decrypted.
t. Data lock: temporary suspension of any processing operation, by keeping personal data or the database;

4 - INFORMATION SECURITY RULES

All information generated, accessed, handled, stored, shared or discarded in the exercise of activities carried out by employees, suppliers, customers, partners and service providers, are the property and exclusive right of use of DNS WOMEN.
DNS WOMEN establishes in its contracts with Suppliers specific clauses of requirements regarding the implementation and maintenance of the LGPD.
DNS WOMEN provides its Security Policy, for the security of its partners, whenever requested.

4.1 . GENERAL ACCESS TO DATA - PRINCIPLES

The company provides all employees and contracted third parties with access to the information they need to carry out their responsibilities effectively and efficiently.
Users are referred to here as holders.
Each holder must be identified by a unique user ID so that individuals can be held accountable for their actions.
The use of shared identities is allowed only where appropriate, such as in training, using only the holder's first name.
Each holder must read this Data Security Policy and the login and logout guidelines and sign a declaration that they understand the conditions of access.
Subject access logs may be used to provide evidence for security incident investigations.

Access should be granted on a need basis, meaning that each program and incumbent will have only the information it needs to complete its tasks.

4.2 ACCESS TO SERVERS AND NETWORK - CONTROL AND AUTHORIZATION

o Access to the company's IT resources and services will be granted through the provision of a unique user account and complex password (created and changed as established by DNS WOMEN).
o Accounts are provided by the IT person based on HR records.
o Passwords are managed by the IT Service Desk.
o Password length, complexity, and expiration requirements are stated in the DNS WOMEN password policy
o Role-Based Access Control (RBAC) will be used to secure access to all file-based resources contained within the active database.
o All employees and contractors must have access to the network in accordance with access control, procedures and the principle of necessity and non-discrimination.
o All employees and contractors who have remote access to company networks must be authenticated using VPN authentication mechanism only.
o Network segregation should be implemented as recommended per current industry best practices on network security.
o Network administrators should group information services, users, and information systems as appropriate to achieve the necessary segregation.
o Network routing controls must be implemented to support the access control policy.
o Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storage and services.

4.3 EMPLOYEE/CONTRACTOR'S RESPONSIBILITY

All employees, contractors and holders in general directly related to DNS WOMEN will have access to the data and applications necessary for their work functions and must, even remotely:
o Lock their screens whenever they leave their desks;
o Keep your workplace clear of any sensitive or confidential information when leaving;
o Keep your passwords confidential and not share them;
o Sign the acknowledgment and obligation to follow this Policy.
o Access to data classified as 'Confidential' or 'Restricted' is limited to authorized employees, whose job responsibilities require, in accordance with this Policy and DNS WOMEN's HR Policy
o Responsibility for implementing access restrictions rests with the IT security officer.
o The Collaborator may only access data from other holders and confidential systems, if there is a commercial need to do so, and only if approval has already been obtained.
o Systems containing sensitive, confidential or restricted data will be physically or logically isolated, and only authorized personnel will be given access.
o Any Collaborator or Contractor, directly related to the internal activities of the company that violates this Policy, will be subject to disciplinary actions, which may include dismissal or contract termination.

4.4 SEALS

The collaborator or contractor, directly related to the internal activities of DNS WOMEN is not authorized to:

- The use of DNS WOMEN's email is for corporate purposes and related to the activities of the employee or contractor within the organization. The use of private email that does not use the @dnswomen.org.br domain for matters related to the interests of DNS WOMEN is not allowed.
- Carry out any type of maintenance or repair on corporate technological resources, except for the IT person in charge;
    - ♣ In case of remote work, requiring maintenance, this must obtain authorization from IT, to safeguard personal data of third parties, if any.
- Using programs that bypass the security controls and controls imposed by DNS WOMEN;
- Execute file sharing programs or different structures that allow interconnection between users from different locations through public networks, except when previously and expressly authorized;
- Access to sites that redirect traffic (proxy) and circumvent digital policies;
- Install, Uninstall or Disable software installed in technological resources by DNS WOMEN, regardless of the reason, except for the person responsible for IT;
- Employees or partners are prohibited from entrusting the safekeeping or sharing of DNS WOMEN's digital certificate to third parties, or using digital certificates from third parties without proper power of attorney;
- Circumvent any security systems;
- Secretly watch others for electronic devices or software;
- Disrupt servers or computer networks through any illegal or unauthorized method;
- Use any type of technological resource to commit or be an accomplice in acts of violation, sexual harassment, disturbance, manipulation, or suppression of copyright or intellectual property without the due legal authorization of the owner;
- Host, access and share pornography, racist material or any other material that violates the legislation in force in the country.
- Using pirated software, an activity considered criminal according to national legislation.
- Carrying out the transfer and/or disclosure of any software, program, or data to third parties, by any means of communication (physical or digital), can only be carried out with the proper identification of the applicant, if positively verified and in accordance with the classification of such information and with the real need of the recipient.
- Store personal and/or non-business files (photos, music, videos, etc.) on network drives, as they can overload server storage. If the existence of these files is identified, they can be permanently excluded, allowing the company to notify the user in advance.
- Use removable information storage devices (pen drives, CDs, DVDs, external hard drives) to transport information. In case of extreme necessity and exceptions, it is necessary to contact the IT responsible for the evaluation of the

case with the responsible manager, if allowed, the device must contain encryption technology. All transported content must be stored on the corporate network and erased from the device immediately after use.

- In case of authorized sharing of documents through mobile storage devices (pen drives, external hard drives, etc.), the media must contain an encryption application with a security level compatible with the Advanced Encryption Standard (AES) or higher.
- Only private equipment authorized by the IT manager can be in remote connections to the DNS WOMEN environment.
- The configuration of this equipment can only be done by the IT manager, obligatorily, with security mechanisms, such as an encryption system, antivirus, tools for secure access to the VPN (Virtual Private Network) and personal firewall, in order to ensure confidentiality and integrity of the information.

4.5 - PHYSICAL STORAGE

Data physically stored with personal data must follow the following procedures to guarantee the security of that data:

- DNS WOMEN follows several norms and best practices regarding document storage and disposal.
- Documents containing personal data are treated as confidential, marked as such and with exclusive access to authorized employees.
- Such documents, when there is an obligation/need to destroy them, must be shredded in appropriate machines.

4.6 – BACKUP

The IT person in charge will create the definitions and execute the specific operational procedures and manuals, according to the characteristics of the information, systems, and backup generation tools, considering at least the following good practices:

- Generation of redundant backups, when necessary, in support of operational contingencies.
- secure and environmentally sound storage with constant updates of security tools.
- use of cryptography
- restriction of access to safeguarded material;
- secure transport of media to remote storage;
- Secure disposal of obsolete, damaged media and backup tools, considering the definitive elimination of their content and, when necessary, the destruction of the physical support.

4.5 INCIDENTS

Those responsible for IT and Security must always work to maintain the best operational practices and adequate tools to avoid security incidents in DNS WOMEN's activities.

The identified occurrence of a state of the system, data, information, service, or network, which indicates a possible violation of this Policy, the LGPD, failure of controls, or previously unknown situation, which may be relevant to information security, are considered incidents and may come from external or internal actions or human errors.

The IT person must prepare a Technical Guide that establishes technical guidelines and specifies the requirements for the technical controls used to grant access to data, allowing an audit of login attempts on any device on the company's network.
The Technical Guide will contain at least the following points:

- Windows NTFS permissions for files and folders (defines what actions users can perform on a file or folder - full control, changes, group/individual)
- (RBAC Model and Access Control) Access control model based on the user's role in the company;
- Server access rights;
- Firewall permissions;
- Use of cookies;
- Network zone and VLAN (Virtual Local Area Network) ACLs (Access Control List);
- Web authentication rights;
- Access rights to the database(s) and ACLs;
- Encryption at rest and in flight;
- Network segregation;
- Physical access to the company (badge, biometrics, renewal frequency, etc.);
- Security monitoring (pen test, DLP (Data Loss Prevention), antivirus. Use of mobile devices and storage;
- Shadow IT (use, justifications, risks…solutions);
- Password Policy and user identity;
- Digital certificate and its use;
- Specifics for remote work.

The following are recognized Incidents that require action:

- loss of services or resource;
- malfunction due to system overload;
- suspected vulnerabilities or non-compliance in systems or services (DDOS -Zero-Day);
- DDOS-type attacks (SYN load; Ping/ICMP flood; UDP flood; NTP Amplification; IP Fragmentation;
- leakage of information from internal or external personal data, stored and processed in the digital environment;
- violations of security procedures;
- access violations.

The Controller must produce daily reports and weekly consolidations in the event of incidents of any nature, which must be immediately dealt with by the IT manager at DNS WOMEN. This report must inform, in addition to the type of incident, the percentage of the problem already resolved.
In the case of high priority Incidents, identified by IT security, these must be immediately escalated to senior management for notification arrangements, depending on the severity of the case and speed of solution. The deadline for notifying the ANPD is 72 hours.

⇒ **Responsibilities in case of incidents:**

- All collaborators, hired directly related to the internal activities of DNS WOMEN, have the primary responsibility of keeping their property information secure and

informing the person in charge or the IT/Security sector of any suspected malfunction of any system;

- The Security manager responsible for the implementation, supervision and coordination of security procedures and systems with regard to specific information resources;
- The Controller – will coordinate the Incident Response Team, together with a senior executive;
- Incident response team: IT infrastructure, Information Security / IT applications, legal, finance and HR staff.

5 - TRAINING

DNS WOMEN values excellence in the execution of its activities, security and data protection being one of them, thus it undertakes that its employees and partners undergo adequate and periodic training in good practices of information security and protection of personal data.

- Annual training on the LGPD and its rules and basic training on information security are mandatory for all employees and contractors involved with DNS WOMEN's internal activities;
- New collaborators and partners receive initial training regardless of collective training when they join DNS WOMEN;
- These trainings will be given by trained professionals who prove their knowledge on the subject.

6- OTHER PROVISIONS

The provisions and requirements of DNS WOMEN related to information security will be presented below:

- Collaborators and partners are aware that DNS WOMEN registers and stores activities (logs), and monitors all access and use of its physical and digital environments, such as capturing images, audio, or video, including for the purpose to protect its assets and reputation and those with whom it relates;
- The logs can also be made available to the authorities, in case of investigation;
- Whenever deemed necessary, DNS WOMEN can audit or inspect the technology resources that interact with its physical or digital environments on its premises or in the case of remote work, request access to them;
- Collaborating members, as they are in different geographic locations, badges are not required, but those responsible for the chapters, when representing DNS WOMEN, must inform that they are collaborating members.
- DNS WOMEN access control and events retain logs (in general via ICANN zoom. Or when via DNS Women zoom and it is possible to audit if necessary;
- DNS WOMEN complies with the principles of ESG, so the printing of documents should be avoided whenever possible, prohibited and the printing of personal data.

7. DISCIPLINARY PROCESS

The employee or partner who violates the safety rules due to illegal, unauthorized, or contrary actions recommended in this Policy, will be subject to the applicable sanctions,

which may vary from verbal or written warning to the termination of the contract for just cause.

8. POLICY BACKGROUND

Each revision of this Security Policy must be controlled in a table like the one described below (Table 1) and stored in a specific file, referring to the version in the footer of this document.

In case of doubt, the collaborator or partner can request the necessary clarifications by email to the DNS WOMEN data manager.

This Policy must be reviewed and updated at intervals not exceeding 2 years, in order to ensure that all technical and legal security requirements implemented are being fulfilled, updated and in compliance with the legislation in force in Brazil as well as GDPR, Privacy Act and related legislations aorund the world about Data Privacy and Data Security.

Table 1

Responsable	
Approved by:	
Related policies	
Storage localization	
Date of Approval	
Date of revision	
Version	

Vanda Scartezini
General Manager