# Information Security Policy

## Contents

## I. THIS POLICY

A. It is the policy of NeuroTest Pty Ltd that information, as defined hereinafter, in all its forms - written, spoken, recorded electronically or printed - will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to collect, process, store and transmit that information.

B. All policies and procedures are documented and made available to individuals responsible for their implementation and compliance. This documentation, which may be in electronic form, will be retained for at least 7 (seven) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation will be periodically reviewed for appropriateness and currency, a period of time to be determined by the management of NeuroTest Pty Ltd.

## II. SCOPE

A. The scope of information security includes the protection of the confidentiality, integrity and availability of information.

B. The framework for managing information security in this policy applies to all NeuroTest Pty Ltd management, its workers, and other Involved Persons and all Involved Systems throughout NeuroTest Pty Ltd as defined below in **INFORMATION SECURITY DEFINITIONS.**

C. This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in **INFORMATION CLASSIFICATION.**

## III. RISK MANAGEMENT

A. A thorough analysis of all information networks and systems owned or used by NeuroTest Pty Ltd will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats - internal or external, natural or manmade, electronic and non-electronic - that affect the ability to manage the information resource. The analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

B. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of any vulnerability.

## IV. INFORMATION SECURITY DEFINITIONS

**Availability:** Data or information is accessible and usable upon demand by an authorized person.

**Confidentiality:** Data or information is not made available or disclosed to unauthorized persons or processes.

**Integrity:** Data or information has not been altered or destroyed in an unauthorized manner.

**Involved Persons:** Every worker at NeuroTest Pty Ltd, no matter what their status. This includes directors, employees, contractors, consultants, external service suppliers, temporaries, and volunteers. Clients and their users (e.g., patients, research participants, etc) are also involved persons.

**Involved Systems:** All computer equipment and network systems that are operated within or by NeuroTest Pty Ltd. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

**Protected Health Information (PHI):** PHI is health information, including demographic information, created or received by the NeuroTest Pty Ltd which relates to the past, present, or future physical or mental health of an individual that identifies or can be used to identify an individual.

**Risk:** The probability of a loss of confidentiality, integrity, or availability of information resources.

## V. INFORMATION SECURITY RESPONSIBILITIES

A. **Information Security Officer:** The Information Security Officer (ISO) is responsible for the development and implementation of prudent security policies, procedures, and controls, subject to the approval of the management of NeuroTest Pty Ltd. The ISO for NeuroTest Pty Ltd also serves the roles of custodian and user management with respect to information security.

Specific responsibilities of the ISO role include:

1. Ensuring that security policies, procedures, and standards are in place and adhered to by NeuroTest Pty Ltd. .
2. Providing basic security support for all systems and users.
3. Advising on the identification and classification of computer resources. See Section VI Information Classification.
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Providing on-going employee information security education.
6. Performing security audits.
7. Reporting regularly to NeuroTest Pty Ltd on the company’s status with regard to information security.

B. **Information Owners:** The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. Ownership does not signify proprietary interest, and ownership may be shared. With respect to this policy, ownership of test data is shared between NeuroTest Pty Ltd and, separately with each of its clients. For the purposes of information security the client will delegate ownership responsibilities to NeuroTest Pty Ltd for any data stored on NeuroTest Pty Ltd systems.

The NeuroTest Pty Ltd has the responsibility for:

1. Knowing the information for which it is responsible.
2. Determining a data retention period for the information, based on appropriate legal advice.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
4. Authorizing access and assigning custodianship.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of information owned by NeuroTest Pty Ltd.
7. Initiating corrective actions when problems are identified.

8. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.

C. **Custodian:** The custodian of information is responsible for the processing and storage of the information. The role of the custodian falls within the responsibilities of the ISO. The custodian is responsible for the administration of controls as specified by the owner. This includes:

1. Administering access to information.
2. Releasing information as authorized by the Information Owner and/or the Information Security Officer for use and disclosure using procedures that protect the privacy of the information.
3. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.
4. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
5. Reporting promptly to the ISO the loss or misuse of NeuroTest Pty Ltd information.
6. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

D. **User Management:** User management is responsible for overseeing their employees' and clients’ use of information, including:

1. Reviewing and approving all requests for access.
2. Initiating security change requests to keep employees' security records current with their positions and job functions.
3. Revoking electronic and physical access to terminated employees and clients that terminate a contract or fail to use their account for a period of 12 months.
4. Providing employees with the opportunity for training needed to properly use the computer systems.
5. Reporting promptly to the ISO the loss or misuse of information owned by NeuroTest Pty Ltd.
6. Initiating corrective actions when problems are identified.

E. **User:** The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.
2. Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.
3. Keep personal authentication devices (e.g. passwords, SecureCards, PINs, etc.) confidential.
4. Report promptly to the ISO the loss or misuse of NeuroTest Pty Ltd information.
5. Initiate corrective actions when problems are identified.

## VI. INFORMATION CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information will be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information is classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report, etc.) must have the same classification regardless of format. The following levels are to be used when classifying information:

### A. Protected Health Information (PHI)

1. PHI is information, whether oral or recorded in any form or medium, that:

   a. is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or health clearinghouse; and

   b. relates to past, present or future physical or mental health or condition of an individual and the provision of health care to an individual; and

   c. includes demographic data, that permits identification of an individual or could reasonably be used to identify an individual.

2. Unauthorized or improper disclosure, modification, or destruction of this information would violate state and federal health information and confidentiality laws, could result in civil and criminal penalties, and cause serious damage to NeuroTest Pty Ltd and its clients, their patients' or their research interests.

### B. Confidential Information

1. Confidential Information is very important and highly sensitive material that is not classified as PHI. This information is private or otherwise sensitive in nature and is restricted to only those with a legitimate and approved need for access.

   Examples of Confidential Information may include: personnel information, key financial information, proprietary commercial information of commercial, system access passwords and information file encryption keys.

2. Unauthorized disclosure of this information to people without a legitimate need for access may violate state and federal confidentiality laws and/or regulations, or may cause significant problems for NeuroTest Pty Ltd, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the Board of Directors.

### C. Internal Information

1. Internal Information is intended for unrestricted use within NeuroTest Pty Ltd, and in some cases within affiliated organizations such as NeuroTest Pty Ltd business or technical partners. This type of information is already widely distributed within NeuroTest Pty Ltd, or it could be so distributed

within the organization without advance permission from the information owner.

Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

2. Any information not explicitly classified as PHI, Confidential or Public will, by default, be classified as Internal Information.

3. Unauthorized disclosure of this information to outsiders is not permitted.

D. **Public Information**

1. Public Information has been specifically approved for public release by ISO of NeuroTest Pty Ltd. Examples of Public Information may include marketing brochures and material posted to web pages.

2. This information may be disclosed outside of NeuroTest Pty Ltd.

## VII. COMPUTER AND INFORMATION CONTROL

All involved systems and information are assets of NeuroTest Pty Ltd and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. **Ownership of Software:** All computer software developed by NeuroTest Pty Ltd employees or contract personnel on behalf of NeuroTest Pty Ltd or licensed for NeuroTest Pty Ltd use is the property of NeuroTest Pty Ltd and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. **Installed Software:** All software packages that reside on computers and networks within NeuroTest Pty Ltd must comply with applicable licensing agreements and restrictions and must comply with NeuroTest Pty Ltd acquisition of software policies.

C. **Virus Protection:** Virus checking systems approved by the Information Security Officer must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

D. **Access Controls:** Physical and electronic access to PHI, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by NeuroTest Pty Ltd. Mechanisms to control access to PHI, Confidential and Internal information include (but are not limited to) the following methods:

1. **Authorization:** Access will be granted on a “need to know” basis and must be authorized by the ISO. Any of the following methods are acceptable for providing access under this policy:

a. *Role-based access:* access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization’s structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

b. *User-based access:* A security mechanism used to grant users of a system access based upon the identity of the user.

2. **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access PHI, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

   a. At least one of the following authentication methods must be implemented:

      1. **Strictly** controlled passwords (Attachment 1 – Password Control Standards),

      2. Biometric identification, and/or

      3. Tokens in conjunction with a PIN.

   b. The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

   c. An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes).

   d. The user must log off or secure the system when leaving it.

3. **Data Integrity:** NeuroTest Pty Ltd must be able to provide corroboration that PHI, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Methods used to support data integrity include:

   a. transaction audit

   b. disk redundancy (RAID)

   c. daily back-up and rapid recovery systems

   d. encryption of data in storage

   e. digital signatures

4. **Transmission Security:** Technical security mechanisms are in place to guard against the unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

   a. integrity controls, and

   b. encryption of data during transmission.

5. **Remote Access:** PHI, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the NeuroTest Pty Ltd and associated networks.

6. **Physical Access:** Access to areas in which information processing is carried out is restricted to appropriately authorized individuals.

   The following physical controls are to be in place:

   a. Mainframe computer systems are installed in an access-controlled area. The area in and around the computer facility affords protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.

   b. File servers containing PHI, Confidential and/or Internal Information are installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

   c. Facility access controls are implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

E. **Equipment and Media Controls:** The disposal of information will ensure the continued protection of PHI, Confidential and Internal Information.

1. **Information Disposal:**

   a. Hard copy (paper, etc) will be shredded.

   b. Magnetic media (hard drives, zip disks, etc.); data will permanently deleted and overwritten a minimum of three times.

   c. CD ROM and Video disks will shredded before disposal.

2. **Accountability:** Records will be maintained of the movements of hardware and electronic media and any person responsible therefore.

3. **Data backup and Storage:** When needed, a retrievable, exact copy of electronic PHI, confidential or internal information/data will be created before movement or disposal of equipment.

F. **Other Media Controls:**

1. PHI and Confidential Information stored on external media (CD-ROMs, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media will be appropriately labeled so as to identify it as PHI or Confidential Information. Further, external media containing PHI and Confidential Information must never be; left unattended in unsecured areas, and must contain data stored in encrypted form, with the exception of unidentifiable summary research data as approved by the ISO.

2. PHI and Confidential Information will not be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless there is a specific need agreed to by the ISO and the devices have the following minimum security requirements implemented:

   a. Power-on passwords

   b. Auto logoff or screen saver with password

c. Encryption of stored data and other acceptable safeguards approved by Information Security Officer

Further, mobile computing devices can never be left unattended in unsecured areas.

3. If PHI or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of NeuroTest Pty Ltd Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with NeuroTest Pty Ltd.

G. **Data Transfer/Printing:**

1. **Electronic Mass Data Transfers:** Downloading and uploading PHI, Confidential, and Internal Information between systems is strictly controlled. All mass downloads of information must be approved by the Owner and the ISO and include only the minimum amount of information necessary to fulfill the request.

2. **Other Electronic Data Transfers and Printing:** PHI, Confidential and Internal Information will be stored in a manner inaccessible to unauthorized individuals. PHI and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

H. **Audit Controls:** Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for six (6) years.

I. **Evaluation:** NeuroTest Pty Ltd requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection.

## VIII COMPLIANCE

A. The Information Security Policy applies to all users of NeuroTest Pty Ltd information including: staff, contractors, consultants, temporaries, volunteers, clients, external service suppliers, and outside affiliates. Failure to comply with Information Security Policies and Standards by staff, contractors, consultants, temporaries, volunteers, clients, external service suppliers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable procedures of NeuroTest Pty Ltd, or, in the case of clients, termination of the license agreement, and in the case of external service suppliers or outside affiliates, termination of the affiliation. Further, penalties associated with state and federal laws may apply.

B. Possible disciplinary/corrective action may be instituted for, but not limited to, the following:

1. Unauthorized disclosure of PHI, Confidential Information or Internal Information as specified in Confidentiality Statement.
2. Unauthorized disclosure of a sign-on code (user id) or password.
3. Attempting to obtain a sign-on code or password that belongs to another person.
4. Using or attempting to use another person's sign-on code or password.
5. Unauthorized use of an authorized password to invade client, patient or research participant privacy by examining records or information for which there has been no request for review.
6. Installing or using unlicensed software on NeuroTest Pty Ltd computers.
7. The intentional unauthorized destruction of information owned by NeuroTest Pty Ltd.
8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

## ATTACHMENT 1

## Password Control Standards

The NeuroTest Pty Ltd Information Security Policy requires the use of **strictly** controlled passwords for accessing Protected Health Information (PHI), Confidential Information (CI) and Internal Information (II). (See NeuroTest Pty Ltd Information Security Policy for definition of these protected classes of information).

Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

### Standards for accessing PHI, CI, II:

Users are responsible for complying with the following password standards:

1. Passwords must never be shared with another person, unless the person is a designated security manager.
2. Every password must, where possible, be changed regularly – (between 3 to 6 months depending on the sensitivity of the information being accessed)
3. Passwords must, where possible, have a minimum length of six characters.
4. Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
5. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
6. When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc…). A combination of alpha and numeric characters are more difficult to guess.

Where possible, system software must enforce the following password standards:

1. Passwords routed over a network must be encrypted.
2. Passwords must be entered in a non-display field.
3. System software must enforce the changing of passwords and the minimum length.
4. System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15 minute timeframe. Lockout time must be set at a minimum of 30 minutes.
5. System software must maintain a history of previous passwords and prevent their reuse.