



Postnet Suite 237, P/Bag X18, Rondebosch, 7700 • Tel: 021 448 3513 • E-mail: info@pansa.org.za •
3b Beach Road, Woodstock, 7925
Website: www.pansa.org.za
Registered Non Profit Organisation: 019-469-NPO
PBO no: 930017636 PAYE no: 7550756755

01 April 2011

DATA AND INFORMATION STORAGE POLICY

This document contains the policies and procedures governing data and information storage for the Performing Arts Network South Africa (PANS A).

PURPOSE

PANS A must protect all information from loss to avoid damage to the organisation, loss of work and other related files and to avoid adversely impacting our partners. The storage of data in scope and access to the same is a critical business requirement.

It is not anticipated that this policy control can effectively deal with a malicious theft or damage to files or hardware on which data is currently stored, or that it will reliably protect all data. Its primary objective is user awareness, and to avoid accidental loss and negligence scenarios.

SCOPE

1. Any employee, contractor or individual with access to PANS A's systems or data.
2. Any device which handles data or information of any kind pertaining to PANS A. Any device which is regularly used for e-mail, web or other work related tasks and is not specifically exempt for legitimate business or technology reasons.
3. Definition of data to be stored
 - All PANS A related files and folders
 - All member information (eg cellphone numbers)
 - Restricted/Sensitive information (eg industry knowledge that is not public)
 - Confidential information (eg personal information relating to employees)
 - IP information

EMPLOYEE REQUIREMENTS

1. Employees need to acknowledge awareness of policies and agree to uphold them
2. It is the employee's responsibility to ensure that all data on their workstations or other hardware is backed up.
3. Employees should maintain current physical and electronic filing system in good order and as per required filing architecture of the organisation
4. All files should be backed-up **weekly** on an external hard drive kept at the appropriate PANS A office in a lockable filing cabinet.
5. All files should be clearly marked according to PANS A filing architecture requirements and stored in a folders clearly designated to the employee
6. All back-ups should be password protected in order to maintain data security as per *Data and Information Security Policy*

National Steering Committee

Erica Glyn-Jones (Chairperson) • Themis Venturas (General Secretary) • Willie Reetsang (Deputy Chairperson)
Kajal Bagwandeem (Treasurer) • Illa Thompson • Frans Sema • Karen Jeynes • Goitsehang Pholo • Deon Lotz



PERFORMING ARTS NETWORK OF SOUTH AFRICA

Postnet Suite 237, P/Bag X18, Rondebosch, 7700 • Tel: 021 448 3513 • E-mail: info@pansa.org.za •
3b Beach Road, Woodstock, 7925
Website: www.pansa.org.za
Registered Non Profit Organisation: 019-469-NPO
PBO no: 930017636 PAYE no: 7550756755

7. Terminated employees or those whose contracts come to an end will be required to return all records, in any format, containing all PANS A or personal information relating to PANS A.
8. You must immediately notify the National Director or their designated authority in the event that a device containing in scope data is lost (e.g. mobiles, laptops, etc).
9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information storage you have a duty to inform the National Director or their designated authority so that they can take appropriate action.
10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled and stored. Seek guidance from the National Director or their designated authority if you are unsure as to your responsibilities.
11. Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car.
12. Data must be stored on only PANS A approved storage devices and transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). PANS A will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with the National Director or their designated authority.
13. Any in scope information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from the National Director or their designated authority.
14. All users are required to notify the National Director or their designated authority if they suspect they are not in compliance with this policy.
15. Should data loss occur as a result of a PANS A employee not adhering to this policy, that employee will be held personally liable.

TECHNOLOGY REQUIREMENTS

1. All devices in scope will have suitable encryption enabled.
2. All users are required to notify the National Director or their designated authority of any device which is lost or stolen.
3. Encryption policy must be managed and compliance validated by the National Director or their designated authority. Each device user must provide a copy of the active encryption key to the National Director or their designated authority.
4. The National Director or their designated authority has the right to access any encrypted device for the purposes of investigation, maintenance or the absence of an employee with primary file system access.
5. The encryption technology must be configured in accordance with industry best practice to be hardened against attacks.
6. All storage related events will be logged and audited by the National Director or their designated authority to identify inappropriate access to systems or other malicious use.

National Steering Committee

Erica Glyn-Jones (Chairperson) • Themis Venturas (General Secretary) • Willie Reetsang (Deputy Chairperson)
Kajal Bagwandeem (Treasurer) • Illa Thompson • Frans Sema • Karen Jeynes • Goitseman Pholo • Deon Lotz