



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 SECURITY POLICY**

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

### **PURPOSE**

PANS A must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our partners. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this policy control can effectively deal with a malicious theft scenario, 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 PANS A device which handles member data, sensitive data, personally identifiable information or company data. 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 protected
  - Member information (eg cellphone numbers)
  - Financial information
  - 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. If you identify an unknown, unescorted or otherwise unauthorized individual in the PANS A offices, or utilising PANS A's systems, you need to immediately notify the National Director or their designated authority.
3. Visitors to PANS A must be escorted by an authorised employee at all times. If you are responsible for escorting visitors you must restrict them to appropriate areas, and not allow them access to devices or files holding in scope information.
4. You are required not to reference the subject or content of sensitive or confidential data publically, or via systems or communication channels not controlled by PANS A. For example, the use of external e-mail systems not hosted or sanctioned by PANS A to distribute data is not allowed.

#### **National Steering Committee**

Erica Glyn-Jones (Chairperson) • Themis Venturas (General Secretary) • Willie Reetsang (Deputy Chairperson)  
Kajal Bagwandeen (Treasurer) • Illa Thompson • Frans Sema • Karen Jaynes • 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

5. Please keep a clean desk. To maintain information security you need to ensure that in scope data is not left on your desk unattended.
6. You need to use a secure password on all PANSOA systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
7. Terminated employees or those whose contracts come to an end will be required to return all records, in any format, containing PANSOA or personal information.
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 security 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. 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 that must be moved within PANSOA is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). PANSOA 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. Should data loss occur, or data leakage into the wrong hands, as a result of a PANSOA 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. General Acceptable Use and security awareness training must require users to notify the National Director or their designated authority if they suspect they are not in compliance with this policy.
3. The AUP and security awareness training must require users to notify the National Director or their designated authority of any device which is lost or stolen.
4. 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.
5. 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.
6. The encryption technology must be configured in accordance with industry best practice to be hardened against attacks.

#### National Steering Committee

Erica Glyn-Jones (Chairperson) • Themis Venturas (General Secretary) • Willie Reetsang (Deputy Chairperson)  
Kajal Bagwandeem (Treasurer) • Illa Thompson • Frans Sema • Karen Jaynes • Goitseman 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. All security 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