NATIONAL NUCLEAR REGULATOR

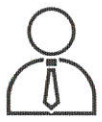
For the protection of persons, property and the environment against nuclear damage

REGULATORY GUIDE

Guidance on implementation of cyber or computer security for nuclear facilities

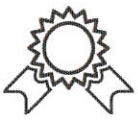
RG-0014

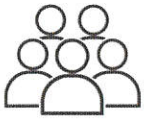
Rev 0


professionalism


integrity


value our people


excellence


teamwork


openness & transparency

UNRESTRICTED

APPROVAL RECORD				
	Name	Designation	Signature	Date
Prepared	BL Ntuane	Chief Inspector: NucSec		23/04/205
	G Pitsoane	Senior Inspector: NucSec		14/04/15
Reviewed	J Boulton	Manager: IT		23/04/2015
	S Tshobeni	Senior Specialist: Electrical Engineering		14/4/15
	U Coetzee	Chief Inspector: NPP		
	P Mohajane	Programme Manager: NORM		14/4/15
	T Pather	Programme Manager: NTWP		5/5/15
	P Bester	Special Nuclear Projects Coordinator		23/4/15
Recommended for Approval by	D Kgomo	Senior Manager: CAE		04/05/2015
	O Phillips	Senior Manager: SARA		8/5/2015
Approved	MB Tyobeka	Chief Executive Officer		5/5/2015

APPROVAL RECORD				
	Name	Designation	Signature	Date
Prepared	BL Ntuane	Chief Inspector: NucSec		
	G Pitsoane	Senior Inspector: NucSec		
Reviewed	J Boulton	Manager: IT		
	S Tshobeni	Senior Specialist: Electrical Engineering		
	U Coetzee	Principal Specialist : SARA		14/4/2015
	P Mohajane	Programme Manager: NORM		
	T Pather	Programme Manager: NTWP		
	P Bester	Special Nuclear Projects Coordinator		
Recommended for Approval by	D Kgomo	Senior Manager: CAE		
	O Phillips	Senior Manager: SARA		
Approved	MB Tyobeka	Chief Executive Officer		

TABLE OF CONTENTS

1 BACKGROUND 4

2 PURPOSE 4

3 Scope/Application 5

4 DEFINITIONS 5

4.1 Abbreviations 5

5 TECHNICAL MEASURES, CHARACTERISTICS AND ATTRIBUTES TO BE ADDRESSED BY LICENSEE AND PROSPECTIVE APPLICANTS 6

5.1 Cyber security policy 6

5.2 The cyber security programme: 6

5.3 Cyber security plan 7

5.4 Protection of Instrumentation, Digital Computer and Communication Systems and Networks 7

5.5 Cyber or computer security office 9

5.6 Cyber security modifications and maintenance 9

5.7 Computer security culture 9

5.8 Reporting of cyber or computer security events or incidents 10

5.9 Review of procedures 10

5.10 Record keeping 10

6 REFERENCES 12

1 BACKGROUND

The overall objective of the cyber or computer security is to prevent, detect and respond to malicious or unauthorised acts directed at nuclear material, radioactive material, associated facilities and activities, as well as providing high assurance that digital computer and communication systems or instrumentation and control systems, and networks are adequately protected against cyber-attacks or unauthorised access to computer based processes and nuclear sensitive information. This is achieved by implementing an effective and efficient cyber or computer security programme which must be able to prevent the successful execution of a malicious act and to prevent and/or mitigate radiological consequences thereof.

The National Nuclear Regulator (NNR) has established the basis for a comprehensive nuclear security regulatory framework in providing regulations and associated technical guidance for authorising nuclear security measures or physical protection systems at nuclear authorisation holders. Cyber security is one of the regulatory aspects within the regulations to which authorisation holders shall comply.

The document assures implementation of cyber security at facilities associated with radioactive material or nuclear material. The guidance is geared towards:

(a) Implementation of security controls to protect the critical digital assets from cyber-attacks;
(b) Application and maintenance of defence-in depth protective strategies to ensure the capability to detect, respond to, and recover from cyber-attacks;
(c) Mitigation of adverse effects of cyber-attacks;
(d) Ensuring the functions of critical digital assets are not adversely impacted due to cyber-attacks;
(e) Ensuring that cyber security implementation does not adversely impact the functioning and performance of systems in nuclear facilities; and
(f) Ensuring that cyber security implementation does not increase system complexity that may adversely affect the operations of nuclear facilities.

2 PURPOSE

The document's purpose is to provide guidance to authorisation holders to implement cyber or computer security on facilities in order to prevent cyber-attacks, sabotage or unauthorised access to critical digital assets and associated infrastructure. It also addresses the potential cyber risks to critical digital assets and provides a flexible programmatic approach in which the licensee or applicant can establish, maintain, and successfully integrate the security controls into a site-specific cyber security program.

3 SCOPE / APPLICATION

The application of cyber or computer security measures should be based on a graded approach on the identified threat or risk assessment of each individual nuclear facility.

4 DEFINITIONS

Unless stated otherwise, terms used in this guide shall take meanings as stipulated below.

"**cyber-attack**" means illegal or unauthorised access on the cyber or computer processes with the intention of or attempting to destroy, expose, alter, disable, steal assets associated with nuclear safety and security control measures.

"**cyber or computer security**" means an aspect of information security concerned with computer-based systems, digital systems and networks.

"**cyber security incident**" means occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a computer based, networked or digital information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent risk of violation of security policies, security procedures, or acceptable use policies..

"**defence-in-depth**" means the combination of successive layers of nuclear security systems and nuclear security measures for the protection of targets from nuclear security threats..

"**need- to- know**" means a principle under which users, processes and systems are granted access to only the information, capabilities and assets which are necessary for execution of the their authorised functions.

4.1 Abbreviations

DBT	Design Basis Threat
EP	Emergency Preparedness
NNR	National Nuclear Regulator
SDOE	Secure Development and Operational Environment
SSEP	Safety, Security or Emergency Preparedness

5 TECHNICAL MEASURES, CHARACTERISTICS AND ATTRIBUTES TO BE ADDRESSED BY LICENSEE AND PROSPECTIVE APPLICANTS

5.1 Cyber security policy

5.1.1 A cyber security policy should be in place and approved by designated Senior Management or Executive Management.

5.1.2 A manager or designated senior personnel should be directly responsible for the policy.

5.1.3 The policy should:

(a) Indicate that the "need-to-know" principle determines controlled access to assets regardless of rank or position in the organisation;
(b) Address security as part of the overall business operation;
(c) Be based on national legal processes or applicable security requirements;
(d) Indicate the responsibilities of different role players involved;
(e) Indicate that all security incidents regardless of their nature be reported to the NNR;
(f) Specify the overall cyber security goals at the facility;
(g) Ensure that cyber security implementation does not adversely impact the functioning and performance of systems in nuclear facilities; and
(h) Ensure that cyber security implementation does not increase system complexity that may adversely affect the operations of nuclear facilities.

5.1.4 Applicable international standards in the policy for the implemented physical protection systems should be indicated and be incorporated by the NNR.

5.1.5 All records and supporting technical documentation required to satisfy the requirements should be retained.

5.1.6 A cyber security policy should be part of the overall facility security policy and should be negotiated and coordinated with other relevant security and safety responsibilities.

5.2 The cyber security programme:

5.2.1 The cyber security program should be a component of the physical security programme

5.2.2 The holder should design a cyber security programme to:

(a) Implement security controls to protect the critical digital assets and nuclear sensitive information from cyber-attacks;

(b) Apply and maintain defence-in-depth to ensure the capability to detect, respond to, and recover from cyber-attacks;
(c) Mitigate the adverse effects of cyber-attacks on safety and security operations;
(d) Ensure the functions of critical digital assets are not adversely impacted due to cyber-attacks;
(e) Sustainability measures to ensure integrity of safety and security control systems; and
(f) Integrate the cyber security program as a component of the physical protection and nuclear safety programme.

5.3 Cyber security plan

5.3.1 The holder should establish, implement, and maintain an effective cyber security plan that:

(a) Describes how the cyber security program shall be implemented
(b) Describes how the holder shall account for site-specific conditions that affect implementation
(c) Includes measures for incident response and recovery during and after a cyber-attack or malicious access to computer processes.

5.3.2 The plan should describe how the holder will:

(a) maintain the capability for timely detection and response to cyber attacks;
(b) mitigate the consequences of cyber attacks;
(c) correct exploited vulnerabilities;
(d) restores affected systems, networks, and/or equipment affected by cyber-attacks; and
(e) implementing a sustainability programme to ensure continuity in adequate safety and security controls.

5.4 Protection of Instrumentation, Digital Computer and Communication Systems and Networks

5.4.1 The holder should:

(a) Identify critical instrumentation, digital or control systems and networks (critical systems) that provide a safety, security, or emergency preparedness capability as well as critical digital assets that are part of, or are connected to ensure nuclear safety and information security.
(b) Analyse instrumentation, digital computer and communication systems and networks and identify those assets that shall be protected against cyber-attacks.

(c) Ensure that instrumentation, digital computer and communication systems and networks are adequately protected against cyber-attacks, up to and including the design basis threat.
(d) Protect instrumentation, digital computer and communication systems/networks associated with:
    (i) Safety-related and important-to safety functions;
    (ii) Security functions;
    (iii) Emergency preparedness (EP) functions, including offsite communications; and
    (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or EP (SSEP) functions.
(e) Protect SSEP systems and networks from cyber-attacks that would:
    (i) Adversely impact the integrity or confidentiality of data and/or software;
    (ii) Deny unauthorised or malicious access to systems, services, and/or data; and
    (iii) Adversely impact the operation of systems, networks, and associated equipment.

5.4.2 Section 6.5.3.7 of PP-0017 (Design and Implementation of digital instrumentation and control for nuclear installations - Rev 0) provides the following additional guidance on digital instrumentation and controls:

The purpose of cyber security is to detect and then eliminate or mitigate vulnerabilities in the digital system that could be exploited either from outside or inside of the digital instrumentation and control system. The process of defending against this class of failures is made more challenging by the rapidly evolving "industry" that continues developing new attack methods. Various individuals and undocumented organisations develop viruses, worms, and associated computer programs. Others concentrate on developing methods for gaining access to protected data and systems with the intent to disrupt system operations or illegally obtain information from the systems.

Authorisation holders have to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks, up to and including the design-basis threat (DBT).

5.5 Cyber or computer security office

5.5.1 The facility should designate a responsible senior official for cyber or computer security management who is a member of Senior Management or Executive Management.

5.5.2 The designated senior official or Senior Management should ensure that cyber security management is part of the strategic plan for reaching corporate goals.

5.5.3 The designated senior official for security management should be the custodian of the facility cyber security plan.

5.5.4 As a minimum the senior cyber security official should account for:

(a) Proper administration of the cyber security programme for the facility and the organisation;
(b) Development and implementation of the facility cyber security procedures; and
(c) Ensuring that cyber security elements are monitored, inspected, maintained, updated and reviewed to provide the required protection levels for the facility, physical protection systems, personnel information and associated nuclear sensitive information.
(d) Full accountability for configuration control of the cyber security systems.

5.6 Cyber security modifications and maintenance

5.6.1 A regular testing and maintenance programme should be established and implemented.

5.6.2 Before any modifications and maintenance is undertaken, the holder should submit the modification or maintenance plan to the NNR. Procedures should be in place for maintenance or modifications on cyber security measures to be reported to the NNR.

5.6.3 Procedures should be in place for all modifications and maintenance on cyber security measures to be authorised by senior management.

5.6.4 Procedures should be in place for vendors providing maintenance or modifications to be authorised by recognised entity.

5.7 Computer security culture

5.7.1 A robust computer security culture is an essential component of any effective security plan. Management should ensure that cyber or computer security

awareness is fully integrated into the overall nuclear security culture programme.

5.7.2 As a minimum, the cyber or computer security culture should ensure that:

(a) Computer security requirements are clearly documented and well understood by staff;
(b) Clear and effective processes and protocols exist for operating computer systems both inside and outside the organization;
(c) Staff members understand and are aware of the importance of adhering to the controls within the computer security programme;
(d) Integrity of nuclear sensitive information and the various components forming the instrumentation and control system is a responsibility for all employees; and
(e) Contractors working on computer and digital systems in the Nuclear Facilities to be sensitised of cyber or computer security protocols.

5.8 Reporting of cyber or computer security events or incidents

5.8.1 Reporting of cyber or computer security events or incidents should be as per section 6 of the General Nuclear Security Regulations.

5.8.2 Attempts to gain unauthorised access or successful hacking into the facility cyber administrative or instrumentation and control processes should be reported to the NNR.

5.9 Review of procedures

5.9.1 Cyber or computer security procedures should be reviewed every 2 years or as and when required to do so.

5.10 Record keeping

5.10.1 Procedures should be in place for cyber or computer security records to be kept for at least 40 years by the licence holder after occurrence of a cyber or computer security event or incident.

5.10.2 Procedures should be in place to ensure that all configuration and maintenance activities of secure computer and digital systems are recorded and such records

be kept for as long as the computer and digital systems are in commission, and these records shall be kept for 10 years after decommissioning such systems.

5.10.3 Records of incidents including testing and maintenance should be documented on-site in accordance to approved management procedures.

5.10.4 Cyber or computer security records should be accessible to authorised and cleared individuals on need-to-know basis.

6 REFERENCES

The following references were consulted during the compilation of this document:

[1] Act No. 47, 1999, National Nuclear Regulator Act
[2] General Nuclear Security Regulations in terms of section 36, of the National Nuclear Regulator Act, 1999 (Act no. 47 of 1999)
[3] PP-0017, Design and Implementation of Digital Instrumentation and Control for Nuclear Installations, Rev 0
[4] IAEA Nuclear Security Series No.17
[5] Convention on the Physical Protection of Nuclear Material (Infcirc 274 Rev.1)
[6] Various International Best Practise Standards.