LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

INCIDENT MANAGEMENT POLICY

Ref: 6/1/P

Date of approval:....13 June 2016

Recommended:

M Labuschagne.................................... 03/06/2016........................

Maisela, RJ Date

(Head of Department)

Approved:

.... 13/06/16........................

Matshoge, BAJ Date

Table of Contents Page

1. Acronyms and abbreviations

GITO	Government Information Technology Office
HOD	Head of Department
IT	Information Technology
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of the Executive Council

2. Executive summary

This policy is aiming to explain the managements of incidents with regards to IT matters within the LDARD. It gives a detailed description of the different categories of incidents and the sensitivity levels. It addresses reporting procedures and refer to extremely sensitive, sensitive and non-sensitive matters. The list of definitions enable all to understand the terminology and the roles and responsibilities are set out clearly.

3. Introduction

An 'Incident' is defined as any event which is not part of the standard operation of a service and which may cause an interruption or reduction in the quality of that service. Incident Management within LDARD is an important aspect of managing information security risk. A security incident may occur from failure of hardware, infrastructure or software; inadequate operational procedures; malicious code; hacking and /or human errors.

4. Purpose and objectives

The purpose of this policy is to preserve the confidentiality, integrity and availability of LDARD electronic information.

The objective of this policy is to provide guidelines and principles to ensure that incidents shall be recorded, reviewed and resolved using an incident management process. Incident response procedures shall be established for each system to include system failures, denial of service and breaches of confidentiality. Corrective action to recover from a security breach and system failure shall be developed so that:

a) Authorised staff is allowed access to systems and data.
b) Emergency actions are documented.
c) Emergency action is reported to management.
d) The integrity of business systems and security controls is confirmed.

5. Authority

This policy is issued under the custodianship of the Accounting Officer and the Honourable MEC for Agriculture and Rural Development in Limpopo.

6. Legal Framework

- SITA Act, of 1998
- Public Service Act, No 103 of 1994

REFERENCES:

- ISO 17799: Section 8.1.3
- CobIT: DS10
- ITIL Book: Incident Management

7. Scope of application

This policy is applicable to all users who make use of LDARD's information resources. All users and staff to whom such resources are available are aware of the policy and act in accordance with it. The policy also applies also to all temporary staff, contractors, service providers, or consultants. All incidents management processes and procedures shall be strictly subject to the provisions of this policy.

8. Definitions

DOS/DDOS:	Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users.
Malware:	Software (or script or code) designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems.
Rootkit:	Stealthy type of malicious software (malware) designed to hide the existence of certain processes or programs from normal methods of detection and enables continued privileged access to a computer.
SPAM:	Also known as **junk email** or **unsolicited bulk email** (**UBE**) is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email.
Trojan:	Software that can make copies of themselves, steal information, or harm the computer system.
Worm:	A self-replicating malware computer program, which uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.

9. Policy Pronouncements

9.1 PRINCIPLES

Information security incidents and malfunctions shall be reported, escalated, resolved, monitored and communicated in accordance with LDARD's Incident Management processes. The following principles shall be adhered to for compliance with policy requirements:

9.1.1 Incident Reporting and Classification

9.1.1.1 Categorizing Incidents

Sensitivity levels vary depending on circumstances.

The following are sensitivity level definitions:

Sensitivity	Level Description
S1	Extremely Sensitive
S2	Sensitive
S3	Not Sensitive

All incidents managed by LDARD should be classified into one of the categories listed in the table below:

Incident Category	Sensitivity Level	Description
Denial of service	**S3**	DOS or DDOS attack.
Forensics	**S1**	Any forensic work to be done
Compromised Information	**S1**	Attempted or successful destruction, corruption, or disclosure of sensitive LDARD Information or Intellectual Property.
Compromised Asset	**S1,S2**	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	**S1**	Theft / Fraud / Human Safety / Child Pornography. Computer-related incidents of a criminal nature, likely involving law enforcement or Loss Prevention.
Internal Hacking	**S1,S2,S3**	Reconnaissance or Suspicious activity originating from inside the LDARD network, excluding malware.
External hacking	**S1,S2,S3**	Reconnaissance or Suspicious Activity originating from outside the LDARD network (Partner network, Internet), excluding malware.
Malware	**S3**	A virus or worm typically affecting multiple LDARD devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan.
Email	**S3**	Spoofed email, SPAM, and other email security-related events.

Policy Breaches	**S1,S2,S3**	A) Sharing offensive material, sharing/possession of copyright material. B) Deliberate violation of Information Security policy. C) Inappropriate use of LDARD asset such as computer, network, or application. D) Unauthorised escalation of privileges or deliberate attempt to subvert access controls.

9.1.1.2 Initial Reporting

All information security related incidents should be reported, in the first instance, to the IT Helpdesk. This will enable the incidents to be logged, investigated, acted on and escalated as appropriate.

The contact details for the IT Helpdesk are as follows.
Telephone: 015 294 3071
Email: helpdesk@agric.limpopo.gov.za

9.1.1.3 Other Reporting Options

In certain circumstances the person wishing to report an incident may be concerned about reporting an incident to IT Helpdesk due to the sensitive nature of the incident. In such cases members of staff may call Anti-Corruption or Fraud Hotline: 0800701701

9.1.1.4 Escalation

Minor incidents of an operational nature will be dealt with by IT Department. These will be summarised in a weekly security operational report to the IT Department but need not be escalated.

If the incident is more serious or deemed to be a breach of policy, security or legislation, this will be reported immediately, by IT Helpdesk to Information Security Office and GITO. The member of staff reporting the incident should also inform their line manager, who will assist in determining what action is appropriate and who needs to be informed and consulted.

9.1.2 Incident Management

9.1.2.1 Extremely Sensitive and Sensitive Incidents

Extremely Sensitive and Sensitive Incidents affecting LDARD shall receive immediate attention. If required, the necessary actions shall be taken to isolate the affected areas. The timeous isolation of affected areas is critical to the business continuity of LDARD. This shall minimise the risk of unaffected areas also being affected by the critical incident and decrease the overall impact on LDARD's information resources.

9.1.2.2 Non-sensitive Incidents

Non-sensitive incidents shall follow current LDARD Helpdesk call logging and resolution procedure.

9.1.2.3 Responding to Incidents

Recorded incidents shall be responded to in accordance with the Incident Management process. Action to recovery from security breaches and to correct system failure shall be carefully and formally controlled. Suitable feedback processes shall be implemented to ensure that the people reporting the incidents are notified of results after the incident has been dealt with and closed.

9.1.2.4 Incident Response and Resolution Procedures

Incident response procedures shall be established to include system failures, denial of service and security breaches. These procedures shall cover:

a) Analysis and identification of the cause of an incident.

b) Assessment of the impact of incidents.

c) Development and implementation of countermeasures to prevent the incident.

d) Review of Audit trails.

e) Discussions with business users and others affected by, or involved with the incident.

f) Provide the respective user or system owner with a unique incident number.

9.1.2.5 Unresolved Incidents

Unresolved incidents shall be made aware and actioned upon. All unresolved security incidents shall be reviewed in order to ascertain what remedial action has been taken.

9.1.2.6 User Awareness

Users shall be made aware of what constitutes an incident, and how to react to these incidents. Users of information resources shall be made aware of the different types of incidents, and the associated incident management procedures. They shall be required to note and report any observed or suspected security weakness in, or threats to, systems or resources. Incidents shall be reported to LDARD Helpdesk as soon as identified.

9.1.2.7 Customer Survey

Users are required to take part in customer surveys to allow the IT Department adequate feedback in order to optimise the processes, procedures or similar functions.

9.2 ROLES AND RESPONSIBILITIES

Issue	Person Responsible	Alternate
Has overall responsibility for adherence to policy	LDARD GITO	LDARD IT Manager
Has the responsibility for implementation and adherence to the policy	LDARD ISO	LDARD IT Manager

10.Default

No deviation from this policy is allowed. Should any deviation be needed, it will only be granted with the written approval of the Accounting Officer – after thorough investigation and motivation.

1) Any attempts to bypass security controls or to obtain unauthorised access or to make unauthorised use of a user account belonging to someone else shall be considered a security violation.
2) The use of LDARD's information assets for purpose other than for authorised business purposes shall be considered a security violation.
3) The use of LDARD information assets for any unauthorised or illegal activity shall be considered a security violation.
4) Any act (or failure to act) that constitutes or causes a security incident or creates a security exposure shall be considered a security violation.
5) Any act (or failure to act) that results in sensitive or business critical information being disclosed to an unauthorised person shall be considered a security violation.
6) Any act (or failure to act) that results in sensitive or business critical information being modified or destroyed such that the LDARD or any of its branches / sub branches is adversely impacted shall be considered a security violation.
7) Any breach of this policy or any of its related documents shall be considered a security

violation.

8) Any person charged with a security violation shall face disciplinary action.
9) All information abuses and security breaches should be reported to the Information Security Officer.

11.Inception date

The date of approval (as indicated on the cover page of this policy) is also the date of inception.

12.Termination and review

This policy should be reviewed every 24 months (2 years) or as and when a need arise.

13.Enquiries

All enquiries regarding this policy should be directed towards:

The Director: IT
Limpopo Department of Agriculture and Rural Development
PO Box 9487
POLOKWANE
0700
Tel: 015 294 3000
E-mail: ITHelpDesk@agric.limpopo.gov.za

Recommended by:

M Labuschagne .... 03/06/2016 ....

Maisela, RJ **Date**

(Head of Department)

Approved by:

.... 03/06/2016 ....

Matshoge, BAJ **Date**

(Hon MEC for Agriculture and Rural Development)