Province of the
EASTERN CAPE
EDUCATION

Directorate ICT

Information Security Policy

Status:	In Draft Under Review Sent for Approval Approved Rejected
Version:	V0.3
Release Date:	22/02/2021

Table of Contents

1) Purpose 5
2) Scope and Applicability 5
3) Policy Principles 5
4) Governance, Roles and Responsibilities 8
4.1) Governance 8
4.2) Roles and Responsibilities for Information Security Management 8
5) Reporting Breaches 8
6) Disclaimer 8
7) Management 8
8) Revision 8
9) Enforcement 9
10) Implementation 9
11) APPROVED/NOT APPROVED 10

A. FOREWORD

This document sets out the INFORMATION SECURITY POLICY to be followed within the Eastern Cape Department of Education (ECDoE) that to seeks to safeguard the ECDoE from Information Security attacks, misuse of information assets and unauthorised disclosure of information.

This policy is a living document and may be amended at any time. Any questions regarding this policy should be directed to the Director: Risk Management

It is important for all staff who are responsible for safeguarding the ECDoE's information, be familiar with this policy.

B. DOCUMENT OWNERSHIP

The Department reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately. A copy of the latest version may be obtained from:

The Office of the Director: Risk Management

Department of Education

Head Office Park, Steve Tshwete Complex

Zone 6,

Zwelitsha

C. REVISION CONTROL

Version	Date
V.0.1	22/02/2021

D. ABBREVIATIONS AND DEFINITIONS

The following abbreviations and definitions are used in this document:

Abbreviation/Definition	Description
Data	Data in this policy deals with any character, text, word or number that has not been processed e.g. employee's ID number.
Endpoint Device	An endpoint device in this policy refers to an internet-capable device on a TCP/IP (Internet Protocol) network. The term can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialised hardware such as POS terminals and smart meters.
Information	Information in this policy is the meaning given to data once it has been processed. It is data that is processed, organised, structured or presented in a meaningful form.
Information Security Incident	An Information Security Incident is the act of violating this Information Security policy, unauthorised use of ECDoE information assets, attempts (either failed or successful) to gain unauthorised access to the ECDoE information assets, unauthorised changes to ECDoE's firmware, hardware, applications or configurations, malicious activities and an alert (system generated) or warning from an individual that there could be a threat to the ECDoE's information or data confidentiality, integrity or availability.
Malware	Malware in this policy refers to programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour.
Operating System	An operating system in this policy is system software that provides a platform for running computer programmes and services.

1) Purpose

The purpose of this policy is to outline the ECDoE's principles and policy statements regarding information security management and ensure all parties are aware of their responsibilities with regards information security management within the ECDoE.

2) Scope and Applicability

This policy applies to all employees, as well as any third parties (such as outsourcing providers, vendors, suppliers, contractors, alliance partners, etc) who have information security related responsibilities or who are responsible for the protection of the ECDoE's information and data. The policy serves to govern information and data as part of responsible internal asset use and good governance within the ECDoE.

3) Policy Principles

In support of this policy, the following principles seeks to safeguard the ECDoE from Information Security attacks, misuse of information assets and unauthorised disclosure of information and data:

Principle	Principle Description	Policy Statements
Information security management must be governed effectively.	Information security management must be governed through suitable leadership and effective governance structures, documented policies, processes and procedures.	• An information security management process must be developed, implemented, adopted, and maintained. • An ICT security services management process, more technically focused, must be developed, implemented, adopted, and maintained. • Information security management must be governed through adequate governance structures. • The ICT Security and Risk Committee must oversee the information security management process implementation and information security related risk matters. • An information security strategy must be developed, implemented and reviewed annually. • Information security management initiatives must be put in place with regular progress reporting as part of the ICT Strategic Plan implementation. • An information security policy, with supporting policies and procedures must be documented. • An information security architecture, that determines the current and future technical standards for information security technology, must be designed and implemented. • Suitable technology must be identified, planned and implemented as part of the information security management process.
Information security related risk must be mitigated effectively.	Information security related risk must be mitigated through an effective information security risk approach and information security compliance measures.	• A formal information security risk management approach must be established in accordance with the ECDoE enterprise risk management framework. • The ECDoE must ensure it complies with legislative, regulatory, contractual or its own internal policies regarding the protection of its information or data. • Annual information security reviews must be conducted on all areas of the enterprise architecture using a risk-based approach and assessment. • Information security controls must be implemented to ensure that information security related risk is mitigated.

Principle	Principle Description	Policy Statements
Information and data must be treated in line with stakeholders' verified requirements.	The ECDoE's information and data must be treated in line with all stakeholders' verified requirements, internal and external, treated with appropriate care and protected adequately to guard against misuse, destruction, inappropriate or wrongful access, disclosure and change.	• Enterprise information and data must be classified in alignment with the ECDoE Data Governance Policy and Standard Operating Procedure. • Personal information or data of customers, stakeholders and staff can only be collected, processed, stored, and disseminated using ECDoE information assets, in order to meet a valid ECDoE business requirement and only after the individual's consent has been obtained. • The ECDoE must monitor and log all aspects of ECDoE communications including, but not limited to, monitoring email by users, monitoring internet usage including public and private cloud services, provided this is monitoring authorised by the ECDoE as set out in the ECDoE Information Security Management Standard Operating Procedure. • During their service with the ECDoE, employees retain proprietary information, data and knowledge. Present and former employees must guard against disclosing or using this information, data and knowledge to the prejudice of the ECDoE's interests. To this end, the ECDoE reserves the right to take action, including legal action, against present and former employees who disclose or use any ECDoE proprietary information or data to the detriment of the ECDoE. • Information and data must be managed, retained and disposed of in line with statutory and business requirements.
Information security operations and technology must enable and protect the ECDoE's strategic business objectives.	The ECDoE's information security operations and technology must enable and protect the ECDoE's strategic business objectives though controls deployed throughout the ICT environment as well as managing human resources and third parties with regards to information security.	• Physical environmental security controls must be adopted to protect ECDoE information and data assets housed in data centres against environmental damage and manage physical access to these facilities. • Information security event management tools must be underpinned with suitable procedures. • Access to the ECDoE network must be managed and controlled to limit inappropriate behaviour. • Cloud security standards must be designed and implemented to decrease the risk of data loss and unplanned downtime. • Password, authentication and privilege standards must be established to prevent unauthorised. • The ECDoE must ensure its information and ICT assets are protected from malware through appropriate technical safeguards. • Business application, operating system and database security standards must be designed and implemented to limit information security attacks. • Measures must be established to ensure ICT assets are managed throughout their lifecycle and to preserve the integrity, availability and confidentiality of enterprise information and data. • An ICT change management process must be designed and implemented to protect the confidentiality, integrity or availability of information resources within the ECDoE. • ICT services must be managed appropriately to ensure that the disruption and loss of production is limited. • Third Parties, including their equipment and services, must be controlled with regards to information security. • Critical third-party services must be managed in a formal service level agreement, that includes the ECDoE's information security service expectations, which must be reported transparently. • Users must use their mobile devices in such a manner that the risks of these devices are minimised. • Storage media must be managed in such a manner that recovery is efficient in the event of a information security related incident.

Principle	Principle Description	Policy Statements
Information security operations and technology must enable and protect the ECDoE's strategic business objectives.	The ECDoE's information security operations and technology must enable and protect the ECDoE's strategic business objectives though controls deployed throughout the ICT environment as well as managing human resources and third parties with regards to information security.	• Information, data and hardware must be retained and disposed of in line with statutory and business requirements. • Appropriate safeguards must be established to prevent unauthorised access to sensitive output documents e.g. payslips, special forms and sensitive reports.
Threats from employees regarding information security must be minimised.	Threats from employees regarding information security must be minimised through appropriate controls and training.	• Appropriate due diligence reviews on all candidates for employment, contractors, and third-party users must be conducted in accordance with relevant laws, regulations and ethics, proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. • An Information Security structure must be established and maintained to ensure clear direction for information security initiatives and visible management support. • All information security roles and responsibilities of employees, contractors and third-party users must be documented in accordance with their duties regarding information security. • Information security training and awareness sessions must be conducted as part of the annual information security awareness programme. • All new ECDoE staff must receive mandatory information security training as part of their induction. • All ICT technical and ICT operations staff must receive training on information security threats and safeguards, and the extent of the training must reflect staff member's individual responsibility for configuring and maintaining information security safeguards. Where ICT staff change jobs, information security needs must be re-assessed, and new training provided as a priority. • All users of new ICT solutions must undergo training to ensure that their use of the system does not compromise information security.

Principle	Principle Description	Policy Statements
Information security related threats, incidents and vulnerabilities must be responded to effectively.	Information security related threats, incidents and vulnerabilities must be responded to effectively through an information security threat detection and incident response capability.	• Information security related incidents such as data breaches, improper conduct or loss or theft of information and data assets must be managed and reported on as part of the information security incident management procedure. • An information security incident response capability must be established that has the necessary ability to deal with information security related incidents. • A proactive information security threat intelligence ability must be established. • Appropriate information security tools must be implemented as defined by business requirements, that protects and monitors the ECDoE environment for information security threats. • An information security vulnerability management and reporting procedure must be developed and implemented

4) Governance, Roles and Responsibilities

4.1) Governance

- The provisions of this policy are intended to be read in conjunction with Information Security Policy Framework and the Information Security Management Standard Operating Procedure, which will be enforced at function level.
- This policy is governed and approved by the ICT Security and Risk Committee.

4.2) Roles and Responsibilities for Information Security Management

- **DEXCO** – Board level. Accountable for protection of information and data.
- **ICT Security and Risk Committee** - Must ensure that an Information Security Management System (ISMS) is developed, implemented and operated effectively. Ensure that the ECDoE's electronic information is adequately protected.
- **Executive Management** - Responsible for protection of information and data.
- **Head of Risk Management** - Overall accountable for Information Security Management. Responsible for carrying out the directives of the ICT Security and Risk Committee with regards to information security. Must ensure that information security related risks are managed.
- **Internal Audit** - Provide independent assurance of the ICT control environment and that the Information Security Management Process is functioning adequately.
- **CIO** - Lead and manage the ICT department. Ensure that ICT complies with the Information Security Management Process and carries out the directives of the ICT Security and Risk Committee
- **ICT Security Management Function** - Must resolve ICT security attacks. Must report to the ICT Infrastructure Manager on ICT security issues and weaknesses.
- **ECDoE Management** - Are responsible for abiding by the ISMS as well as any relevant security policies laid out in the ISMS.
- **ICT Management** – Jointly responsible for implementing Information Security Management in their areas to support the ECDoE' information security objectives.

5) Reporting Breaches

Any breaches of this policy must be promptly reported to ICT Service Desk offices at 040 608 4779 or email to ITSupport@ecdoe.gov.za.

6) Disclaimer

""Eastern Cape Department of Education (ECDoE) assumes no liability for direct and/or indirect damages arising from the user's use of ECDoE's information assets. The ECDoE is not responsible for any third-party claim, demand, or damage arising out of the use of the ECDoE's information assets."

7) Management

Ownership of this policy falls to the Director: Risk Management. For any questions about this policy please contact him/her at 040-6084244.

8) Revision

- The ICT Security and Risk Committee is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.
- An internal audit will be performed annually to ensure that the policy is properly aligned with ECDoE objectives and that performance is meeting established triage parameters.

9) Enforcement

- It is the responsibility of all relevant ECDoE managers of operating units to ensure that these policies are clearly communicated, understood, and followed by the relevant staff for whom they are responsible.
- Any user or staff member found to have violated this policy may be subject to disciplinary action as described in the Department's Code of Conduct and Disciplinary Procedures including revocation of his/her computer account, suspension, or termination of employment, or civil or criminal prosecution.
- A procedure for enforcing this policy must be developed and implemented by Risk Management.

10) Implementation

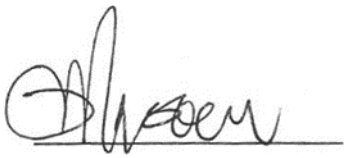
- A policy implementation schedule is given below:

Activity	Month 1	Month 2	Month 3	Month 4	Month 5-12
Communicate policy to key stakeholders.					
1st approved version of policy.					
Policy Awareness Workshops.					
Acknowledgement of understanding signed by all ECDoE.					
Incorporate policy into existing processes and procedures where required e.g. staff take on.					
Develop enforcement procedure.					
Implement enforcement procedure.					
Perform internal audit of policy to determine conformance.					
Conduct quarterly compliance reports to committee.					

11) APPROVED/~~NOT APPROVED~~

_____

_____



22/02/221

Mr. Tshepo Maseou. **Date**
Chairperson: ICT Steering Committee