ICT POLICY	
Document No	CSIR-MS-POL-ICT-001 REV02
Revision Status	02
Prepared by	Arthur A. Madonsela Chief Information Officer (CIO)
Last Review Date	29 January 2019
Effective Date	09 April 2019
Approved by	CSIR Board
Date Approved	09 April 2019
File Plan Number for Related Records	1/2/1

TABLE OF CONTENTS

1. DOCUMENT CHANGE HISTORY 4
2. DEFINITIONS 5
3. LIST OF ABBREVIATIONS 7
4. PURPOSE 8
5. SCOPE 8
6. OBJECTIVES 8
7. EFFECTIVE DATE 8
8. REFERENCE DOCUMENTATION 9
9. COMPLIANCE WITH POLICY 9
10. EXEMPTIONS 10
11. ROLES AND RESPONSIBILITIES 10
    11.1. CSIR Board 10
    11.2. CSIR Board's Audit and Risk Committee (ARC) 10
    11.3. CSIR Executive Management (Exco) 11
    11.4. CSIR Management 11
    11.5. Chief Information Officer (CIO) 11
    11.6. Employees 11
12. POLICY STATEMENTS 11
    12.1. ICT Management 11
    12.2. ICT Organisation 11
    12.3. ICT for Business Use 12
    12.4. Personally-Owned ICT Resources 12
    12.5. ICT Asset Management 12
    12.6. Privileged or Administrative Rights 12
    12.7. Protection of Information 12
    12.8. Information Systems Acquisition, Development and Maintenance 13
    12.9. Systems Planning and Acceptance 13
    12.10. Physical and Environmental 13
    12.11. Backup and Recovery 13
    12.12. Third-party Management 14
    12.13. ICT Service Continuity Management 14
    12.14. Change Management and Release Management 14
    12.15. Availability and Capacity Management 14
    12.16. Configuration Management 14
    12.17. Service Management 14
    12.18. Problem and Incident Management 15
    12.19. Cloud Services 15

12.20. Mobile Services 15
12.21. ICT Hosted Services 15
12.22. Knowledge Management 15

1. DOCUMENT CHANGE HISTORY

PUBLICATION DATE	AUTHOR	REVISION NO	CHANGE DESCRIPTION
17 February 2011	Arthur A. Madonsela	01	Board Approved Policy
21 January 2019	Arthur A. Madonsela	02	Revised with relevant changes as advised by PRDC (05 December 2018) and OPCO (16 January 2019) and EXCO (28 January 2019)

2. DEFINITIONS

Term	Definition
Acceptance criteria	Defined and measurable terms of what must be done for an information system to be acceptable to affected users or employees, especially in terms of functionality
Access control	A process or control through which access is restricted to authorised individual users, applications, third parties or information systems.
Availability	Ensuring timely and reliable access to and use of information.
Best practice	Recommendations or solutions that are considered the most desirable or preferred.
Business Continuity Management (BCM)	A management process followed to identify risks, threats and vulnerabilities that can impact the CSIR's continued operations and provides a framework for building resilience and the capability for an effective response and/or recovery. Matters of ICT service continuity management are considered a key aspect of this process.
Business Continuity Plan (BCP)	A plan detailing measures, procedures, controls and/or arrangements used by an organisation to respond to the disruption of critical business processes and services. It is dependent on the disaster recovery process or plan for restoration of critical systems.
Classification	The act or process by which data and/or information is determined to be of a particular category or class.
Confidentiality	The principle that information is not made available or disclosed to unauthorised individuals, entities or processes.
Data	A set of values, numbers, characters, words or other elements that may be interpreted or processed in order to produce information.
Disaster	An unplanned event causing great damage or loss of information resources or the capability to perform certain functions.
Disaster Recovery Process/Plan	A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
Electronic Communication	Any text, voice, sound, image, or video message sent over an electronic network, such as e-mail, instant message (IM), SMS, WhatsApp, BBM message, unified communication and video conferencing.
Employee	For the purpose of this document only, the term employee is considered to include all permanent and/or temporary individuals employed or appointed by the CSIR.
Event	An occurrence of or change in a particular set of circumstances.
Fourth-party	A person or entity associated with the Third-party.
Guideline	A document that provides recommended but not mandatory advice regarding practices in a given situation, scenario or topic.
Incident	An identified occurrence of an adverse event, indicating a possible breach of policy, failure of controls, or previously unknown situation that may have an impact on the information security and privacy responsibilities of an organisation.
Incident Management Process	A formal documented set of steps or instructions in order to be able to respond, to mitigate, or handle an incident and the consequences thereof.
Information Asset	An information asset is a valuable or useful object, which includes:

	• Technology assets (databases, data files, electronic documents, software, development tools and utilities) • Physical assets (computer equipment, communications equipment, or computer media)
Information Processing Facility	Any information system, service, infrastructure or the physical location that they are housed in.
Information Resource	Any data/information in electronic, physical, verbal or audio-visual form or any hardware, software or information processing facilities that makes possible the use, handling, transfer and/or storage of data/information.
Information System	An application, service, information technology asset, or any other information handling component.
Information System Lifecycle	A process for planning, creating, testing, implementing, maintaining and retiring an information system.
Information Security	All measures taken to protect the confidentiality, integrity, availability, resilience, authenticity and non-repudiation of information resources. The scope of information security includes cybersecurity.
Information Security Management System	Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.
Information Security Policy	A set of statements which express management's intent for the implementation, maintenance, and improvement of its information security.
Integrity	The property of information that describes its accuracy and completeness, especially as impacted by unauthorised modification.
ICT Organisation	Formally approved ICT service entity/structure that includes, but not limited to, management, staff, processes, etc; as it is organised to service the CSIR
ICT Service	A means of delivering value to the business by facilitating the achievement of the outcomes and objectives of the business These are typically provisioned through the user of ICT infrastructure, business application systems etc.
Least Privilege	Giving an employee only those privileges that are essential for the employee's role/function.
Management	Employees who are responsible for managing the organisation, and/or functions or people within the organisation. These individuals are often responsible for setting the strategy of the organisation or function, and for coordinating the efforts of its employees to accomplish its objectives through the application of available resources, such as financial, natural, technological, and human resources.
Mobile Device	A handheld, portable computing device which includes, but is not limited to, cell phones, smart phones, tablets.
Must	An action/control that is mandatory.
Need-to-Know	The principle that restricts access to information resources only to those who require access to that information in order to perform their [job] responsibilities.
Personal Device	Refers to electronic equipment that has a processing capability and is owned by an individual/employee and is not owned by the

	CSIR. Often this refers to a desktop, laptop, tablet or smartphone.
Procedure	A series of activities or tasks that contribute to the fulfilment of a task.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event.
Sensitive (critical) Role	A role identified as being vital to the organisation, and the compromise of which will endanger the effective functioning of the organisation.
Service Level Agreement	Specific responsibilities of the service provider, including the satisfaction of any relevant information privacy/security requirements, and sets the customer's expectations regarding the quality of service to be provided.
Standard	A document that provides specific, low-level mandatory controls that help enforce and support policies.
Supplier Agreement	A document that is used for an appointment of a third party to provide services to an organisation.
Third-party	A person or entity other than the CSIR and its Employees
Threat	A circumstance or event that has the potential to exploit vulnerabilities and violate information security.
Transfer	The sending and/or sharing of information.
Unauthorised Access	Gaining access to an information resource without permission.
Vulnerability	A lack of or weakness in the design, implementation, operation of a control that could expose information resource to threats or risks.

3. LIST OF ABBREVIATIONS

Abbreviation	Full term
4IR	Fourth Industrial Revolution
ARC	Audit and Risk Committee
BCM	Business Continuity Management
BCP	Business Continuity Plan
Board	The CSIR Board
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technologies
CSIR	Council for Scientific and Industrial Research
DRP	Disaster Recovery Process/ Plan
ECT	Electronic Communications and Transactions Act 25 of 2002
ICT	Information and Communications Technology
IP	Intellectual Property
IS	Information Security
ISO	International Organization of Standardization
ITIL	Information Technology Infrastructure Library (IT Service Management Framework)
MISS	Minimum Information Security Standards
POPIA	Protection of Personal Information Act 4 of 2013
PRDC	Policy Review and Development Committee
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
SLA	Service Level Agreement

4. PURPOSE

The purpose of this policy is to articulate the CSIR's position on the use of Information Communication and Technology (ICT) information systems, resources and services, as well as the CSIR's expectation for the management and operations of such during the course of business operations.

Equally important, the policy is intended to align ICT investments and service activities to the enablement and support of the CSIR Business Strategy.

5. SCOPE

This ICT policy applies to all CSIR employees including permanent, temporary, Third-party contractors, Fourth-parties, consultants, auditors, interns, and studentship holders of the CSIR who have access to and make use of the CSIR ICT information systems, resources and services, and/or personal devices that contain CSIR information or are used to access ICT business services.

This ICT policy is supported by and must be read in conjunction with the other CSIR policies and standards, including but not limited to, the CSIR Information Security Policy, Privacy Policy, and Acceptable Use Standard.

6. OBJECTIVES

The objectives of this policy are to ensure that ICT delivers value to the CSIR; through:

i. Optimal, efficient and effective usage of ICT to improve the CSIR's performance and competitiveness, as well as support the business strategy, goals, objectives and requirements
ii. Ensuring the integrity, reliability, availability, and expected performance of the CSIR ICT applications, systems and related infrastructure
iii. Understanding and management of the risks, benefits and constraints resulting from the utilisation of ICT within CSIR
iv. Provision and implementation of appropriate governance regime(s) in line with applicable codes of governance practice
v. Compliance with applicable ICT-related legislation, regulations, rules, codes and standards

7. EFFECTIVE DATE

This policy is valid from the "Effective Date" outlined herein and is valid until further notice.

8. REFERENCE DOCUMENTATION

This document is in support of or is supported by, amongst others, the following:

Number	Reference	Name of the Regulation /Document
1.	**CSIR Policies/ Documents**	Conditions of Service
2.		Information Security Policy
3.		Information Privacy Policy
4.		Acceptable Use Standard
5.		CSIR Approval Framework
6.		Procurement Policy
7.		Intellectual Property and Technology Transfer Policy
8.		Records Management Policy
9.	**Regulatory Framework**	Scientific Research Council Act (Act No 46 of 1988)
10.		The National Key Point Act, 1980 (Act No. 102 of 1980)
11.		Public Finance Management Act (Act No.1 of 1999 as amended by Act 29 of 1999)
12.		The Regulation of Interception of Communications and Provision of Communication-related Information Act (Act No. 70 of 2002) ("RICA")
13.		Promotion of Access to Information Act (Act No.2 of 2000)
14.		Electronic Communications and Transactions Act (Act No 25 of 2002)
15.		Disaster Management Act (Act No. 57 of 2002)
16.		The National Strategic Intelligence Act (Act No. 39 of 1994)
17.		Electronic Communications and Transactions Act 25 of 2002 (ECT)
18.		Protection of Personal Information Act 4 of 2013 (POPIA)
19.		Minimum Information Security Standards (MISS)
20.	**Best Practice**	COBIT 5 (Control Objectives for Information and Related Technologies) – ISACA IT Framework
21.		ITIL (Information Technology Infrastructure Library) IT Service Management Framework
22.		ISO 9001 – Quality management systems – Requirements
23.		The King IV Code on Corporate Governance

9. COMPLIANCE WITH POLICY

All CSIR employees must comply with this policy and supporting standards, processes, procedures and guidelines. Failure and/or refusal to abide by this policy may be deemed as misconduct, which may result in an investigation and/or disciplinary action against an employee, grounds for termination of a contract or refusal by the CSIR to enter into a contract. *A claim of ignorance as to the existence and/or application of this policy cannot be grounds for justification of non-compliance.*

If any provision of this policy is rendered invalid under law, such provision must be deemed modified or omitted to the extent necessary, and the remainder of this policy must continue to be enforceable and in full effect.

While the CSIR respects the privacy of its employees, it reserves the right to audit and/or monitor their handling of, or activities on, its information resources. It further reserves the right to monitor and/or audit the content of any information stored, processed, transmitted or handled by employees using the CSIR's information resources and/or personal devices that contain CSIR information.

Where the CSIR has reasonable grounds to suspect that its information security has been/is being compromised and/or the information security policy has been breached, the CSIR reserves the right to:

- Intercept and peruse any data sent, received, or stored by any employee (including any attachment to it) and to monitor the use of its information resources, including, but not limited to, Internet access, email use, hard drives, network drives, and other computing systems; and
- Conduct inspections of the information resources without advance notice to all employees.

10. EXEMPTIONS

Exemptions, exceptions or deviations from this policy will only be considered insofar as they are lawful and do not compromise the CSIR's legal obligations and duties. Approval for exemptions, exceptions or deviations from this policy, if warranted and lawful, must be submitted in writing for approval by the Board or by delegation to EXCO.

11. ROLES AND RESPONSIBILITIES

The roles and responsibilities associated with this policy are outlined below. These roles and functions shall be responsible for collaboratively giving effect to the organisational, operational processes and technology aspects required by the CSIR to drive compliance with this ICT policy throughout the organisation. More details on the specific roles, responsibilities, activities and tasks related to ICT are defined and documented in supporting standards and approved documents.

Management must review these roles and responsibilities periodically, and whenever there is a change in the legislative or regulatory landscape which may have an impact on ICT operations and activities, and update the policy accordingly.

11.1. CSIR Board

With respect to this policy, the CSIR Board is responsible for:

i. Approval of the ICT policy.

11.2. CSIR Board's Audit and Risk Committee (ARC)

With respect to this policy, the CSIR Board ARC is responsible for:

i. Providing oversight for the effective implementation of the ICT policy.

11.3. CSIR Executive Management (Exco)

The CSIR Exco is responsible for:

i. Ensuring that an effective ICT policy has been documented and implemented.
ii. Reviewing and recommending the ICT policy for CSIR Board approval.

11.4. CSIR Management

i. Executives, managers, supervisors and/or any person mandated with the responsibility to manage staff must understand the ICT policy requirements as they apply to their areas of responsibility and must ensure that their staff discharges their ICT responsibilities accordingly.

11.5. Chief Information Officer (CIO)

The CIO of the CSIR is responsible for:

i. The development and implementation of any ICT strategy, policies, standards, processes, procedures as may be necessary for compliance with this policy or any legal obligations
ii. Assessment and management of ICT risks

11.6. Employees

i. All employees (as defined in the Definitions) must take responsibility for protecting their own and the CSIR's information assets.
ii. All employees must understand and comply with the provisions of this ICT policy as well as supporting ICT standards, processes and procedures. Where required, ICT responsibilities must be included and documented in job roles and responsibility descriptions.

12. POLICY STATEMENTS

The policy statements below describe the appropriate controls and mechanisms that must be put in place to adequately support the CSIR's business operations. These policy statements are aligned with generally accepted practices for ICT.

12.1. ICT Management

In order to ensure that there are appropriate and effective ICT controls and mechanisms across the CSIR, ICT management must ensure alignment of services with business requirements and these services must support the delivery of the business strategy, goals, objectives and requirements at all times.

12.2. ICT Organisation

Provisions must be made to ensure that the ICT organisation, and supporting capabilities and resources (people, process and technology), are adequately capacitated to support the overall delivery of the CSIR business strategy, goals, objectives and requirements.

Additionally, roles and responsibilities for various ICT functions must be clearly defined, documented and communicated. Where certain ICT services or functions are decentralised or shared across the CSIR, such responsibilities must be clearly defined to minimise ambiguity or unnecessary duplication of effort or resources.

12.3. ICT for Business Use

The use of CSIR ICT services are primarily for business purposes. The CSIR allows limited personal use of its information resources, however, in order to protect its business interests it may monitor, audit, examine or investigate the use and content of its information resources. To this end, employees should be aware that any expectation of privacy they have while using the CSIR's information resources is limited.

12.4. Personally-Owned ICT Resources

Employees who choose to make use of personally-owned devices for CSIR business purposes connect to consume CSIR information resources or business services must comply with the relevant policies and standards. Bearing in mind that where a personally-owned device is authorised for use of business services, the ICT support of that device will be on a "best effort" basis.

12.5. ICT Asset Management

In order to ensure adequate and efficient control of ICT assets, the standardisation and management of all ICT resources, the reduction of total cost of ownership and a streamlined ICT support service, the acquisition of all ICT assets (hardware and software including licenses) must be facilitated by the ICT Services Centre in line with the CSIR Procurement Policy. Mechanisms and structures must be put in place to manage the standardisation of ICT and related information assets where possible.

Additionally, software installed on any CSIR ICT asset must only be installed following formal authorisation to do so, and must be done in strict compliance with the applicable license(s) and/or associated agreements.

12.6. Privileged or Administrative Rights

All employees will be granted basic/standard user access rights to CSIR information resources in accordance with the principal of "least privilege". Where privileged or administrator rights are required, a formal process for requesting these rights must be followed. Such rights and entitlements must be reviewed on a periodic basis, and removed when no longer required. The CSIR may remove such rights or entitlements in the event of misuse.

12.7. Protection of Information

All devices, whether CSIR or personally-owned, which store or have access to CSIR information or business services must have the necessary information protection

controls (such as encryption) required to safeguard the information. Where this is a CSIR-owned device, these safeguards must be implemented and managed by the ICT Services Centre.

Specifically, employees are prohibited from making use of forensic software or any other tools which may attempt to defeat or circumvent controls or otherwise destroy CSIR information stored on a CSIR-owned device.

12.8. Information Systems Acquisition, Development and Maintenance

To ensure that information systems are managed across their entire lifecycle a formal information system acquisition, development and/or maintenance process must be documented and implemented.

12.9. Systems Planning and Acceptance

To ensure that all business requirements are considered as an integral part of the development, procurement and maintenance of information systems used by the CSIR, Business, user and functional requirements must be defined and incorporated into the architecting, design and planning of an information system from its initiation.

Additionally, key stakeholders must be identified at the onset of the project or initiative. Acceptance or production criteria must be defined for all new information systems, upgrades and/or new versions or releases, and must be met prior to the acceptance and rollout of the information system. An assessment against all requirements must be completed and accepted by stakeholders before an information system can be accepted as production ready.

12.10. Physical and Environmental

In order to ensure the correct operations of the CSIR's information resources, all information systems must be installed within an appropriate facility that meets the requirements of that information system; and all ICT equipment and all related physical infrastructure and environmental equipment must be correctly maintained and operated.

12.11. Backup and Recovery

In order to protect the CSIR's information resources against loss and/or damage and to ensure that information resources can be recovered if they are lost and/or damaged, all information resources, that the CSIR requires to carry out its daily operations, must be securely backed up at appropriate intervals. This includes, but is not limited to, applications, operating systems, databases, hardware and software configurations, log files, and any other relevant data.

12.12. Third-party Management

In order to protect the CSIR information resources accessible to or services provided by third parties, and to maintain an agreed level of control and service delivery in line with service level agreements (SLA) and/or supplier agreements, a contract must be entered into between the CSIR and all third parties providing ICT services to or having access to any of the CSIR's information resources, to ensure that the CSIR's interests are protected and that all CSIR requirements have been contracted between both parties.

12.13. ICT Service Continuity Management

In order to ensure that the CSIR has the ability to restore the availability of information resources in a timely manner, ICT service continuity management plans, processes and procedures must be developed and maintained in order to ensure that there are service continuity measures and contingencies in case of an adverse event, and to ensure that information resources are sufficiently resilient. ICT service continuity requirements must be addressed within the CSIR's overall business continuity plans and processes, and must align with the CSIR Information Security Policy and any other relevant Policies.

12.14. Change Management and Release Management

Change and release management controls and mechanisms must be in place to govern all changes to CSIR's information systems, ensure that ICT changes are implemented in a controlled manner and minimise the likelihood of undesired disruptions of business operations as a result of information system changes.

12.15. Availability and Capacity Management

Controls and mechanisms must be in place to ensure that ICT services and solutions are optimised to meet existing and future availability, performance and capacity requirements and demands. Processes must be defined to continuously identify and address ICT service availability as well as capacity requirements and concerns.

12.16. Configuration Management

Controls and mechanisms must be in place to ensure that documentation related to the design and configuration of information systems is documented, approved and maintained.

12.17. Service Management

Controls and mechanisms must be in place to ensure that ICT services are aligned with business requirements and expectations and that these services are rendered in alignment with agreed/defined operating and service level agreements. These agreements must be monitored and reviewed on a regular basis.

12.18. Problem and Incident Management

To ensure a consistent approach to the management of ICT problems and incidents, an ICT problem management regime (i.e. approach and relevant processes) must be implemented and maintained in order to ensure that recurring problems and incidents are addressed in a timely and organised manner.

12.19. Cloud Services

While acknowledging the potential benefits of using cloud services, the CSIR processes and stores sensitive information, some of which is of national importance. For this reason, the use of cloud services for storing, handling, transferring and/or the processing of CSIR information will require authorisation from the CSIR Exco; provided it does not contravene any applicable laws and regulations, or other CSIR Policies.

12.20. Mobile Services

ICT will develop and roll-out Mobile Services for CSIR Employees, in order to enable Employees to execute their operational responsibilities remotely on a need basis or as and when necessary. Employees who require access to the Mobile Services will follow internal management approval to obtain access to the Mobile Services. Upon approval, the Employees will when utilizing the Mobile Services, take into account all CSIR's relevant policies and procedures relating to information security, safety, HR, Finance, etc.

12.21. ICT Hosted Services

Where there is a requirement for non-CSIR information systems or ICT services to be hosted at, managed and/or operated by the CSIR, a thorough risk assessment must be completed before authorisation to initiate the project is granted.

Specifically, no contract involving the hosting of third-party ICT services shall be entered into without the involvement of and approval by the relevant CSIR stakeholders.

12.22. Knowledge Management

Knowledge management practices must be in place to ensure that a culture of knowledge-sharing is embedded into the organisation and that knowledge is continuously improved to support in the provisioning of services.