



---

**Circular No H 224/ 2021**

**TO: ALL HEADS OF DIVISIONS/ CHIEF DIRECTORATES/ DIRECTORATES/ DISTRICTS/ REGIONS/  
INSTITUTIONS/ SUB STRUCTURES**

As we are becoming increasingly dependent on the use of IT systems and the threat of cyber security breaches becoming more real, the diligent management of user access to our systems becomes all the more important. This includes, amongst others, the approval of new users, the regular six-monthly review of existing users, the management of passwords and the management of the termination process of employees who exit the Department from an IT perspective.

***The primary responsibility of the above-mentioned processes lies with every line manager.*** You are therefore called upon to please comply with the attached policy with immediate effect. It includes an executive summary and provides the more detailed guidance and requirements in this regard.

.....  
Dr Krish Vallabhjee  
CD: Strategy  
Date: 31 December 2021



# Western Cape Government:

## Department of Health- ICT Systems Policy

### Document Properties

Title		ICT Systems Policy for Department of Health, WCG.
Name		<ul style="list-style-type: none"> <li>WCG, DOH ICT Systems Policy</li> </ul>
Document		<ul style="list-style-type: none"> <li>CD: Strategic Cluster</li> </ul>
Owners		<ul style="list-style-type: none"> <li>Director: Information Technology</li> </ul>
Document Date		<ul style="list-style-type: none"> <li>30   12   2021</li> </ul>
Electronic File Name		<ul style="list-style-type: none"> <li>DOH ICT Systems Policy V3</li> </ul>
Electronic Document Location		<ul style="list-style-type: none"> <li>DOH ECM MyContent</li> </ul>
Manual Store		<ul style="list-style-type: none"> <li>Office of the Director: Information Technology</li> </ul>

Document enquiries can be directed to: Department of Health, Information Technology, Western Cape Government, Private Bag x659, Cape Town, 8000, South Africa.

Attention: Director: Information Technology

Email: [sibusiso.mkhonza@westerncape.gov.za](mailto:sibusiso.mkhonza@westerncape.gov.za) | Telephone: +27 (21) 483 8801 | Fax: +27 (21) 483 3277


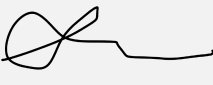

## Document Control Version History

## Document Control:

Last signed Version: 1.2 signed dated 02 | 12 | 2019

Version	Description	Author	Revised Date	Change & Conditions
V 2.1	Draft	Natasha Roodt	30   11   2021	6.2 POPI insert 6.3 Information Security insert 7.4 Digital Processes insert 7.5. Inserts for system review section 10. Procedural deviation during emergencies / Pandemic insert Various inserts to include digital processes with the use of digital signatures
V 2.2	Draft	Natasha Roodt	02   12   2021	Formatting
V 2.3	Insert	Krish Vallabhjee Natasha Roodt	09   12   2021	Inserts for record keeping and disposal requests. Administrator-action insert for de-registration of users.
V2.4	Final Draft	Sibusiso Mkhonza	22   12   2021	Formatting Directorate name change
V 3	Finalised Document	Natasha	30   12   2021	Executive Summary

## Approval Panel

Name	Designation	Version	Date	Signature
Dr Krish Vallabhjee	Chief Director: Strategic Cluster	V3	31/12/2021	
Mr. Sibusiso Mkhonza	Director: Information Technology	V3	31/12/2021	
Ms. Natasha Roodt	Deputy Director: ICT Governance	V3	30/12/2021	

**WARNING: PROPERTY AND COPYRIGHT.**

This document contains confidential information that belongs to the Western Cape Government (WCG). No part of the content may be used, copied, disclosed or conveyed in whole or in part to any party in any manner whatsoever other than the intended purposes without prior written permission from the **Western Cape Government**.

**All copyright and intellectual property herein vests with the Western Cape Government.**

---

**Document Distribution List**

This document is distributed to:

- 1) All WCG Health Staff and Management.
- 2) Department of the Premier: Centre for e-Innovation (Cel)

The Distribution group is required to further distribute the document to relevant WCG and external stakeholders.

### Definitions and Abbreviations

WCG	Western Cape Government
DOH	Department of Health
ICT	Information Communication Technology
IT	Information Technology
DotP	Department of the Premier
TAPS	Transversal Applications Support
CEI	Centre for e-Innovation
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information
COBIT	Control Objectives for Information and Related Technology
MIOS	Minimum Interoperability Standards
MISS	Minimum Information Security Standards
Business Systems Owner	A WCG: Health staff that has a Business Application or proposes to have one.
System Manager	A WCG: Health employee that is responsible/has special rights for the executing administration tasks on business application/s within the WCG: Health.
System Controller	A WCG: Health employee that is responsible/has special rights for executing administration tasks on business application/s within the department.
Organisation/ Department	WCG: Health
PC	Personal Computer
P&P	Policies and Procedures
End-User	Employee, Contractor, Consultant, Service Provider, Agent, or Members of the public who has access to and uses WCG: Health ICT Applications.
Lapsed User Account	A state of User Non-Activity, in which a User's account cannot be accessed without an account Administrator's intervention.
Closed/Disabled User Account	A state in which a User's account is no longer connected to any system. This state renders the account incapable of being used to access the internet, intranet, e-mail, office applications, as well as business applications.

Access Type

A Users account that enables a User to authenticate to a business application and to be granted Authorisation to access resources provided by or connected to that business application.

## Contents

1. Executive Summary .....	7
2. Purpose .....	8
3. Rationale.....	8
4. Scope .....	8
5. Legal framework .....	9
6. Guiding Principles .....	9
7. Policy Statement .....	9
_7.1 General .....	9
_7.2 POPI .....	10
_7.3 Information Security.....	10
8. Policy Content.....	10
_8.1 Access Authorisation and User Account Management.....	10
_8.2 Business Application Requirements for User Access Management .....	14
_8.3 Forms. ....	16
_8.4 Digital Processes.....	16
_8.5 ICT Systems Security Management .....	16
_8.6 Password Management.....	17
9. Multiple Workstation Signings. ....	18
10. Penalty for Transgressions   Deviations. ....	19
11. Deviations During Emergency   Pandemic Periods.....	19
12. General System User Guidelines .....	20
13. WCG Policies and Guidelines. ....	20

## 1. Executive Summary

The Western Cape Government, Health (WCGH) has developed an ICT Systems Policy which is revised annually or as required.

The policy is aligned to WCG policies, adopted governance frameworks, DOH processes, POPI and AGSA required controls for increased service enablement and minimal risk. The target audience for this policy is DOH ICT Users, Line Managers of users, System Administrators, being any user who has administrative rights on a system, and those contracted to provide goods and services which involve access to DOH ICT equipment and systems.

The policy covers detailed processes for user access management for a User, Line Manager, System Administrator and Contractor. These processes include becoming a user, access right amendments, password management, ICT security, terminations, and general ICT user rules. Some processes are manual where forms, emails and telephonic conversations suffice while other processes are embedded in an automated, digital processes.

Business units are the accepted custodians and primary users of systems; and therefore decide who in their environment should have access to systems. The suggested approval structure may be used for required authorisations.

COVID-19 experiences have proven that at times it could be difficult to strictly follow processes described in a policy. Deviation from the normally required processes include telephonic requests supported by an email, process delays with a written confirmation of a plan to complete required processes, and the acceptance of an authorised person forwarding requests on behalf of another user.

It is important that there is alignment between IT and the organisation (business) needs to enable efficiency. To ensure alignment, we continually review and assess the DOH ICT Systems Policy.



## 2. Purpose

The purpose of the policy is to ensure that there is proper use of Information and Communication Technology (ICT) end user systems of the Western Cape Government: Health, therefore any person working with WCG Health information and information technology resources shall comply with this policy.

This ICT Policy Procedural Manual provides the policies and procedures for use of ICT Systems within the DOH, which must be followed by all staff. It also provides guidelines how the WCG: Health will use the policy to administer these ICT systems, providing the correct procedure to follow, The ICT policy should be kept current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

## 3. Rationale

This policy enforces the requirements of the Public Service Regulations with regards to Electronic Government and the governance measures implemented for ICT and Information Technology (IT).

The following sectors are applicable:

### **Public Service Regulations.**

Chapter 5 | Electronic Government Regulations:

Part (i) Underlying electronic government value.

Part (ii) Information Security.

Part (iii) Interoperability.

This policy is a subset of the WCG ICT Policy and therefore does not supersede nor replace the WCG ICT Policy but will enhance its applicability and will always reference the WCG ICT Policy.

## 4. Scope

This policy is applicable to all WCG: Health Divisions, contractors and agents who act on behalf of WCG as end users with regards to the management and use of the Computer Software Systems, Application Systems, Operating Systems, WCG: Health Web Interfaces, Security Systems, equipment, infrastructure and/or any WCG: Health ICT digital collateral.

## 5. Legal framework

This policy subscribes to:

- COBIT 5 Framework
- Electronics Communications and Transactions Act (Act No 25 of 2002)
- Minimum Information Security Standards
- National Health Normative Standards Framework of Interoperability in eHealth in South Africa version 2.0 of March 2014.
- Policy on Ordinary and Advance Electronic Signatures in the Western Cape Government
- Promotion of Access to Information Act (Act No 2 of 2000)
- Protection of Personal Information Act (Act No 4 of 2013)
- Public Service Act (Act No 103 Of 1994)
- Public Service Regulations with regards to Electronic Government.
- SACSA/090/1(4) "Information Security in the RSA"
- WCG ICT Policy

## 6. Guiding Principles

The primary purpose of the ICT Systems Policy is to protect the WCG: Health, Officials, Contractors and any other spheres of Government, and all other parties from illegal or damaging actions or use of ICT Systems, whether deliberate or unintentional. Therefore, the ICT Systems Policy guideline principle is that all WCG: Health ICT Assets should be used for the purposes of the WCG: Health.

This policy provides guidelines for the protection and use of information technology assets and resources within the WCG: Health to ensure integrity, confidentiality and availability of data and assets.

Implementation of this policy provides an added benefit of increased cyber security by ensuring authorized access and processes with built-in preventative measures.

## 7. Policy Statement

### 7.1 General

The WCG: Health is governed by a broad range of legislation regulating Information Communications Technology including, but not limited to, The Electronics Communications and Transactions Act, 2002, and the Regulation of Interception of

Communications and Provision of Communication-Related Information Act, 2002, (The Interception Act).

**Users are bound by all relevant Legislation and Policies** regulating telecommunications, transactions and Information Communications Technology and will undertake at all times to act in accordance with all relevant legislation and policies. Users acknowledge that they have been granted access by the organisation to information and communication technology and resources, including e-mail and internet access. The sole reason for issuing such access to Users, would be to perform duties and responsibilities in accordance with their job function or other official purposes of the WCG: Health.

**Users acknowledge** that they have **No Expectation of Privacy** when utilising any ICT equipment and resources operated under the auspices of the WCG: Health and permission is granted to the WCG: Health to intercept, monitor, read, filter, block or otherwise act upon any electronic telecommunication, stored file or indirect communication which is or has been under their control, received by them or transmitted by them as contemplated in the RICA Act.

## 7.2 POPI

In alignment with the POPI Act 4 of 2013, all personal data is to be treated as confidential. Health data is sensitive and contains personal information of patients. WCG: Health staff data on systems contain personal information which should be treated as confidential. Processing of information must comply with the conditions in the POPI Act 4 of 2013.

## 7.3 Information Security

All users accessing WCG information shall preserve the confidentiality, integrity, and access to information. Security incidents must be reported in accordance with the incident management procedure.

## 8. Policy Content

### 8.1 Access Authorisation and User Account Management

#### 8.1.1 New User Access Authorisation:

Line managers shall authorise New User Access Registration Requests either digitally on the implemented platform for new user applications or using a New User Registration Form which must be made available by the System Manager. The New User

Registration digital or manual form must be completed in full with all mandatory information requirements, which must be signed electronically or manually and authorised.

#### 8.1.2 Approval and Authorisation

**Approval Process:** The ICT Systems Manager must view the digital application or receive a completed form, signed and authorised by the users' Line Manager requesting system access. The request will be reviewed by the system manager for processing and updating the system with the request, whereby the request should preferably be actioned electronically where possible for evidential archival purposes.

#### 8.1.3 Provisioning Criteria on Request for Approval

The End-User shall supply all the mandatory indicated requirements on the form such as Name, Surname, Persal/Contract/ID Number, Access Type and Job Title, which will also include the requesting managers details and authorisation. The internal approval criteria and process at a Facility or Institution must apply when the Users line manager authorizes the account creation on the form.

#### 8.1.4 User Account Allocation

No User Account shall be allocated without an authorised and approved digital application or form being received and processed.

The ICT System Manager/ System Controller/Administrator shall create the User account and allocate logon credentials to the user, which shall then be made known to the requesting user, only.

The User shall replace the logon credentials provided with one that conforms to the standards set in section 7 (Password Management), of this document.

**8.1.5 Issuing User Privileges and Permissions:** The ICT Systems Manager shall be responsible for the approval of processing requests and the Systems Controller/Administrator shall execute the operation or task. (Where allocation or granting of access is mentioned, it shall be implicit that the ICT System Manager shall be responsible for the approval granting access)

8.1.6 **The Allocation of Access**, must be based on a competency, skill or job function.

8.1.7 **End-User Personnel**, shall not gain access to change application software code or any operable or functional architectural structures of the system and development staff shall not gain access to update client data in the live or production environment.

8.1.8 **New User Training for Access Enablement**, Prior to the New User being allocated with access to a system, orientation must take place and evidentiary proof must be available.

8.1.9 **All User Account Status Change Requests**, requesting a revision to privileges shall be processed by either completing a digital request on the implemented platform or a User Privileges Change Request Form in full, provisioning all the mandatory information requirements, which must be signed as authorised by a line manager or mandated senior manager.

The authorising manager shall submit an account status change request either digitally or on a manual form if there is a change in the employee's status, which would require an alteration to the User Account Privileges or closure of the User Account, if they resign or move to another division in the WCG.

The authorising manager must complete the specific systems **De-Registration digital process or Form** for every DOH system, to which the user had access and submit the form to the system manager for processing.

The line manager must complete an IT Request form and stipulate User De-Registration for all the items on the list applicable to the user and submit the request to CEI at [ceiservicedesk@westerncape.gov.za](mailto:ceiservicedesk@westerncape.gov.za)

Access rights associated with any new or revised user access credentials as outlined in 7.1.6 and 7.1.8 above shall all be applicable.

The ICT System Manager / System Controller / Administrator shall ensure that de-registration, according to submissions for terminated users is processed accordingly.

#### 8.1.10 User Account Lapse and Termination

Temporary User Accounts that have an expiration date shall automatically be disabled on the expiration date unless an extension is requested by the Line Manager before the expiration date.

User Accounts that have no activity for 45 consecutive days shall lapse and considered to be a dormant account. These user accounts will be suspended.

All user accounts that have been suspended will be disabled on the system if there is no written communication to re-instate the user account status. Suspended accounts which have not been verified in the bi-annual user review will also be disabled.

- 8.1.11 **Transient Users**, such as temporary or external users must agree to display honest, ethical and professional conduct while collaborating in business with and using the WCG: Health ICT systems, whereby all compliance structures within the policy shall apply to all external users who should be made aware of the obligation of compliance to the ICT Policy.

On receipt of request for a Transient User Account from the Line Manager, the ICT System Manager shall create an account and document the start and end dates to the account of a consultant, contractor, or service provider.

Should the contract be extended, the Line Manager shall submit a request for access extension to the ICT Systems Manager, who shall then update the affected User Account with the new expiry date.

- 8.1.12 **User Groups**, by virtue of their characteristics and allocated privileges, can bequeath similar privileges to all members of the group, therefore be cautious and cognoscente when managing Group Privileges.

- 8.1.13 **User Account Holders** have an **obligation** and **responsibility** for the account management and adherence to confidentiality of their user account, login credentials and must always ensure compliance with the ICT Systems Policy, whereby all users

entering the employment or rendering a service to the WCG: Health shall be made aware of the obligations below.

No end-user shall disclose their login credentials to another.

Accounts shall not be used for private and or commercial purposes.

Report any ICT System misuse or transgressions to your line manager or systems manager.

## **8.2 Business Application Requirements for User Access Management**

8.2.1 All business units within the WCG: Health are the custodians and primary users of the business application systems; therefore, it is the responsibility of the incumbent business units to authorise access to their respective applicants.

8.2.2 The managers in all divisions shall determine who of their employees should be granted access authorisation. They shall decide upon the level and type of access each employee shall obtain. In these decisions the manager shall be guided by the roles and responsibilities defined for each employee.

8.2.3 Development staff shall be granted access to the development environment (where development and applications testing can be accomplished with no risk of impact to production data). Development staff shall be granted a "Read Only Access" to the production environment.

8.2.4 ICT personnel who are not involved in any way with application software development or maintenance shall not be granted access to the development environment without the approval of the systems manager.

8.2.5 Below is a structure that each business, institution, or facility could follow as a guideline regarding the approval structure to obtain certain types of User Access across the WCG: Health, ICT systems.

Table 1- Proposed Institutional Internal User Approval Structure

<i>Chief Director</i>	Can authorise throughout the entire Portfolio of Directorates and Issue non WCG Vendors   Partners Access.
<i>Director</i>	Can authorise throughout the Directorate and Issue External Collaborators and non WCG partners access to that Division, in an instance of a stand-alone service or operation.
<i>Multiple Directors within a Directorate</i>	Can only govern the permissions within their Unit but can co-sign collaboration permissions across Directorate workspaces. The Directors would require approval from the Chief Director.
<i>Deputy Director</i>	Can Authorise throughout the sub-directorate Unit and must request permission from the Director to provide non WCG Collaborators Access.
<i>Multiple Deputy Directors</i>	Can only govern the permissions within their Division but can co-sign collaboration permissions across divisional workspaces. The Deputy Directors would require approval from the Director.
<i>Assistant Director</i>	Can Authorise throughout a Business Unit Workspace that they are specifically responsible for and can collaborate with Multiple Assistant Directors but must request approval of the Deputy Director.
<i>SAO</i>	May request a permissions update on a content level within a Unit Workspace.
<i>The Designated User</i>	Apply the Privileges at the level of Permissions that could be issued to the User or Group.



**8.3 Forms,** The System Manager shall ensure that all User Forms and Controls are available for annual auditing. Records are to be kept for one (1) calendar year after which permission must be requested for disposal.

8.3.1 New User Access | Registration Form:

8.3.2 User Status Change Request Form:

8.3.3 User De-Registration Form:

8.3.4 Password Reset Controls:

**8.4 Digital Processes,** The System Manager shall ensure that audit trails and other digital records for users and changes are available for annual auditing. Records are to be kept for one (1) calendar year after which permission must be requested for disposal.

## **8.5 ICT Systems Security Management**

8.5.1 **System Manager | System Controller | Administrator and User Account Reviews.**

- (1) The System Controllers/Administrators shall review all User Accounts bi-annually, viz. Period 1 being April to September with a review in October and period 2 being done October to March with a review being done in April.
- (2) The System Manager shall review All System Controllers/Administrators User Accounts bi-annually, viz. Period 1 being April to September with a review in October and period 2 being done October to March with a review being done in April.
- (3) The Manager shall review the System Managers Accounts bi-annually, viz. Period 1 being April to September with a review in October and period 2 being done October to March with a review being done in April.

### 8.5.2 Systems Login Violation Report.

- (1) All login security violations, be they intentional, unintentional, or otherwise, must be reported to the ICT Systems Manager.
- (2) The System Controller/Administrator shall review system violations quarterly and issue a standard security violation report for the attention of the Systems Manager.
- (3) The System Managers shall inform the responsible Managers from the different Business Units regarding any Security Violations.

**8.5.3 Output Reports** | All classified output reports must be handled with confidentiality and sorted according to their level of classification, and which shall always remain the property and intellectual capacity of the WCG.

**8.5.4 Security Levels** | Users shall always and only transact with the prescribed Authorised Privileges on any ICT system issued to a User, which is owned and endorsed by the WCG: Health.

**8.6 Password Management** | Passwords are personal identification codes used as keys to gain access into a system, it is the responsibility of the End-users to keep their password confidential, whereby under no circumstances shall the End-users divulge this information to any individuals.

#### 8.6.1 Password Composition and Size

- (1) A password must be created with a combination of Alphabetic, Numeric and Special Characters to ensure a high level of password security.
- (2) Minimum complexity – passwords should use all of the characteristics below.
  - Upper-case Alphabetic character.
  - Lower-case Alphabetic character.
  - Numeric Character.
  - Special Character, such as: !@#\$%^&\*(
- (3) Minimum length of the password must be 6 characters.

- (4) Maximum length of the password must be 14 characters.
- (5) Personalisation of passwords made of Names, Date of Birth, Telephone Numbers, or addresses must be avoided.
- (6) The Password shall not be the same as the logon Identifier.
- (7) The password is Case Sensitive.
- (8) The System Password Lock-Out Threshold should be a minimum of 3 attempts and maximum of 5 attempts before the user account is locked.

#### 8.6.2 Password Duration.

- (1) A password requires a number of unique instances before an old password may be re-used, this number should be 5.
- (2) With the creation of a New User Account or on Resetting an existing user's password, the System Controller/Administrator shall allocate a temporary password, whereupon the User will immediately be informed thereof.
- (3) The User must change the temporary password at the first sign on, whereby the temporary password will expire in the timeframe set by each DOH system.
- (4) A User Password update change is required within 72 days.
- (5) The User must log a call using the controls put in place by the ICT Manager, Centre for Electronic Innovation (CEI) and Transversal Applications Support (TAPS) when requesting a password reset.

#### 9. Multiple Workstation Signings | End Users must be prevented from logging on to multiple workstations at the same time.

**10. Penalty for Transgressions** | Deviations from the Norms and Standards set out in this Policy will constitute a dereliction on the part of the End-user, in such cases the appropriate corrective, disciplinary or punitive action shall apply.

### **11. Deviations During Emergency | Pandemic Periods**

The processes described in this section is only applicable in cases of national or provincial emergency and during periods of pandemic, such as urgent needs occurring after hours and during COVID-19, when it becomes difficult or impossible to follow the normal policy procedures.

**11.1 Telephonic Requests** | The System Manager shall ensure that telephonic requests for new users; changes to user privileges and permissions; de-registrations and/or password resets is supported by an email which contains the user's name and a description of the request. The user's Line Manager or a senior member of staff who is authorized to verify such a request should be included in the email. In cases where a form is used in the normal procedure, this email can be regarded as a replacement for the form.

**11.2 Requests on behalf of users** | In the case where users are unable to request for a password reset or anything else required, the Operational Manager or ward clerk is authorized to do the request on behalf of a user. The request should be done via email with the relevant user included in the email request. If the request is done telephonically, a supporting email needs to follow describing the request with the relevant user included.

**11.3 System Review Timelines** | In cases where system reviews, i.e. user review, System Controller reviews and System Manager reviews; cannot be performed in the normal periods, period 1 being for April to September and period 2 being for October to March, the System Manager needs to inform the ICT Governance Office in writing. The communication needs to confirm the type of review being delayed, person(s) and/or facilities affected, reason for delay and the planned date to resume the required review(s).

**11.4 DRP Testing at Medical Facilities** | It is accepted that while facilities are in a lockdown state and/or focusing on health service tasks during emergency or pandemic periods, DRP testing would need to be postponed. System owners need to inform the ICT Governance Office in writing of the planned date to resume the required annual DRP testing.

## 12. General System User Guidelines

- (1) Do Not write down passwords.
- (2) Do Not include passwords in a non-encrypted stored document.
- (3) Do Not divulge your passwords to anyone, including IT Staff.
- (4) Do Not reveal your passwords telephonically.
- (5) Do Not hint to your passwords format.
- (6) Do Not use the "Remember Password" feature offered in different Browsers.
- (7) Do Not use your corporate or network password on a User Account via the internet, which does not have a secure login, the web address should start with **https://** and not **http://**
- (8) Report any suspicion of Password theft to the IT Helpdesk on 021 4834800.

## 13. WCG Policies and Guidelines

<b>Policies</b>
<a href="#">Anti-Virus Policy.pdf</a>
<a href="#">Asset Management Policy.pdf</a>
<a href="#">Backup and Restoration Policy.pdf</a>
<a href="#">Compliance Policy.pdf</a>
<a href="#">Communications and Operations Management Policy.pdf</a>
<a href="#">E-mobility Data Card Policy.pdf</a>
<a href="#">Policy on Ordinary and Advanced Electronic Signatures in the WCG.pdf</a>
<a href="#">Information Systems Acquisition Development and Maintenance Policy.pdf</a>
<a href="#">IT User Account Management Policy.pdf</a>
<a href="#">WCG Enterprise Information Security Policy.pdf</a>
<a href="#">WCG Human Resources Security Policy.pdf</a>
<a href="#">WCG IT End User Policy.pdf</a>
<a href="#">WCG IT Password Policy.pdf</a>

<a href="#">WCG Online Content Policy</a>
<a href="#">WCG Physical and Environmental Security Policy.pdf</a>
<a href="#">WCG Social Media Policy.pdf</a>
<b>Frameworks</b>
<a href="#">WCG Information Security Framework.pdf</a>
<b>Charters</b>
<a href="#">WCG Security Charter.pdf</a>
<a href="#">WCG Charter for the Corporate Governance of IT.pdf</a>
<b>Circulars</b>
<a href="#">Premier SCM&amp;A Circular No 5 of 2018_Personal Mobile Device Policy.pdf</a>
<b>Documents</b>
<a href="#">CeI Structure April 2018.pdf</a>
<a href="#">2015 CEI Report Perception Survey.pdf</a>
<b>Standards and Guidelines</b>
<a href="#">Anti-Virus Standard.pdf</a>
<a href="#">WCG Business Requirement Specification Guidelines.pdf</a>
<a href="#">WCG Enterprise Naming Standards.pdf</a>
<a href="#">WCG Product Catalogue 2018</a>
<a href="#">WCG ICT Standards v8.3 Nov 2018</a>
<a href="#">WCG Information Security Incident Management Standard.pdf</a>
<a href="#">WCG MSL Reference Guide v2016-18(c).pdf</a>
<a href="#">WCG Logical Access Control Standard.pdf</a>
<a href="#">WCG MS SQL Database and MS Database Engine (MSDE) Security Standard.pdf</a>
<a href="#">WCG Survey Monkey Usage Guidelines.pdf</a>
<a href="#">Writing for Humans</a>
<b>Forms and Templates</b>
<a href="#">DITCOM Reporting Template.pdf</a>
<a href="#">Enterprise Architecture Request Form.doc</a>
<a href="#">Standard Changes and Service Application Form</a>
<a href="#">Mobile Device Policy Application Form.docx</a>
<a href="#">Mobile Device Policy Claim Certificate.doc</a>
<a href="#">WCG Social Media Access Application.pdf</a>
<a href="#">WCG Software Solution Evaluation Form.docx</a>
<a href="#">WCG Software Solution Evaluation Form.docx</a>

