

ENTERPRISE Systems STANDARDS, POLICIES, AND GUIDELINES

II. Windows Environment

1.0 Purpose

To establish requirements which shall be met by all computers connected to the Orange County government network to ensure effective operating system and system integrity.

2.0 Scope

This policy applies to all Orange County government computers running any version of the Microsoft Server Operating Systems. This includes, but is not limited to, servers, workstations and all other appliances with server operating systems that are connected to a network.

3.0 Policy

3.1 General

- 3.1.1 Installations of Business Applications Software required for non-production environments shall be hosted in a virtual environment. Possible Exceptions are:
 - 3.1.1.1 Business Applications with high network traffic or high disk utilization.
 - 3.1.1.2 Servers requiring expansion cards.
- 3.1.2 Server load shall be calculated based on total concurrent users; not possible users.
- 3.1.3 Operating System Software shall be installed on RAID 1 (mirrored drives).
- 3.1.4 The C: Partition shall be equal or greater than 20GB.

3.2 Software Selection

- 3.2.1 Business Application Software, Business Application Data, and IIS shall not be installed on the C: partition.
- 3.2.2 Business Application Data shall be SAN attached.
- 3.2.3 Databases (i.e. SQL) shall not reside on the same server as the Business Application Software or IIS.
- 3.2.4 Business Application Vendors shall support backups/restores using Orange County's Enterprise Backup Tool. Currently, Orange County's standard is CommVault's Galaxy iData-Agents.
- 3.2.5 Business Application service accounts shall not be a member of the domain administrators group.
- 3.2.6 Business Application support staff, including vendors, shall be added to the local administrators group for installations and upgrades. Upon completion of business application software installation, local administrator accounts will be removed.
- 3.2.7 If the Business Application Vendor is allowed to access the server, the Business Application Vendor shall comply with Orange County's Change Management Policies.
- 3.2.8 Business Application Software shall run as a service. Business Applications that require a user account to remain logged in to a server shall not be approved.

3.3 System Requirement – Hardware

- 3.3.1 Servers shall be rack mounted.
- 3.3.2 Servers shall have dual power, dual NIC's, dual processors, and dual HBA's (if SAN attached).
- 3.3.3 Servers shall have a minimum of 4 GB of RAM and two (2) 72 GB hard drive.
- 3.3.4 The following table lists, in order of preference, the currently approved models for purchase:

Virtual Server on ESX Host	Dell Blade (currently PowerEdge 1955)	Dell 1U (currently PowerEdge 1950)	Dell 2U (currently PowerEdge 2950)	Dell 4U (currently PowerEdge 6850)
Preferred	If application does not work in VM environment or Application is too hardware intensive for VMWare (to be determined by OC ISS VMWare Team.	If dedicated NIC's are required (ie connection to content switch)	If add-on cards (ie HBA's) or a large amount of local storage is required	If 4 processors are required (ie ESX Host)

4.0 Guidelines

4.1 These standards, polices, and guidelines shall be followed.

5.0 Enforcement

5.1 Exceptions to the guidelines shall be considered if overriding justification is provided. Upon Orange County's considerations of the overriding rationale, exceptions may be approved and a waiver may be granted.

ENTERPRISE Systems STANDARDS, POLICIES, AND GUIDELINES

III. Oracle Environment

1.0 Purpose

To establish requirements which shall be met by all business application software installed on any computers connected to the Orange County government network to ensure effective database operation and database integrity.

2.0 Scope

This policy applies to all Orange County government computers running any version of the Oracle Relational Database Management System.

3.0 Policy

3.1 General

- 3.1.1 Orange County supported Oracle versions are Oracle Enterprise Edition 9i and 10g with 10g being the preferred version.
- 3.1.2 Orange County supported environment for Oracle databases is UNIX, running on an IBM AIX supported OS.
- 3.1.3 Database setup shall be compliant with Oracle's OFA (Optimal Flexible Architecture – file naming conventions)
- 3.1.4 Business Application Software shall be install under separate schema not requiring DBA privileges or DBA type privileges.
- 3.1.5 Business Application Software shall not require or use the Unix Oracle account.
- 3.1.6 Business Application Software shall provide a security module to manage user ids and permissions.
- 3.1.7 Business Application Vendors shall provide all database creation scripts and any other required scripts to build, maintain and support the database environment.
- 3.1.8 Business Application Vendors shall provide all documentation related to all database creation scripts and any other required scripts to build, maintain and support the database environment. (General item number 3.1.7)
- 3.1.9 Business Application Vendors shall supply initial database sizing requirements (1st yr). Prefer sizing figures for 1^{yr}/3yr/5yr view.
- 3.1.10 Installations of Databases shall be performed by Orange County's staff using vendor provided scripts, initialization parameters, and any special performance related parameters.
- 3.1.11 Business Application Vendors shall identify all Oracle versions and products to which their applications are certified to run on.
- 3.1.12 **Business Application Software/Vendor shall not be required to operate using the Oracle's Administrator (SYSADM) account. NOTE: If SYSADM privileges are required for installation, an Orange County Database Administrator shall perform the installation vendor supplied scripts under the Business Application Vendor's direction.**
- 3.1.13 If the Business Application Vendor is allowed to access the server, the Business Application Vendor shall comply with Orange County's Change Management Policies.
- 3.1.14 Business Application Vendors shall support application database backups/restores through Oracle's backup tools.

4.0 Guidelines

- 4.1 These standards, polices, and guidelines shall be followed.

5.0 Enforcement

- 5.1 Exceptions to the guidelines shall be considered if overriding justification is provided. Upon Orange County's considerations of the overriding rationale, exceptions may be approved and a waiver may be granted.

ENTERPRISE Systems STANDARDS, POLICIES, AND GUIDELINES

IV. SQL Server Environment

1.0 Purpose

To establish requirements which shall be met by all business application software installed on any computers connected to the Orange County government network to ensure effective database operation and database integrity.

2.0 Scope

This policy applies to all Orange County government computers running any version of the SQL Server Relational Database Management System.

3.0 Policy

3.1 General

- 3.1.1** Orange County Supported Microsoft SQL Server versions are Server 2000 and 2005 (Standard or Enterprise Edition) with SQL Server 2005 being the preferred version.
- 3.1.2** Database installations shall be on a separate server from the application executables and support files.
- 3.1.3** Business Applications executables and/or supported files shall not be installed on the C: drive of the Windows Server. The Business Application installation program shall allow the Orange County Database Administrator to specify the drives and directories where the database files will reside.
- 3.1.4** Business Applications Software that only support the MSDE or SQL Server Express Editions shall not be permitted.
- 3.1.5** Business Application Software shall support SQL Servers Integrated Security model.
- 3.1.6** Business Application Software shall contain a security module to manage user ID's and permissions. No blank or hard-coded passwords shall be allowed.
- 3.1.7** Business Application Software/Vendor shall not be required to operate using the SQL Server System Administrator (sa) privileges account.
NOTE: If sa privileges are required for installation, an Orange County Database Administrator shall perform the installation vendor supplied scripts under the Business Application Vendor's direction.
- 3.1.8** If the Business Application Vendor is allowed to access the server, the Business Application Vendor shall comply with Orange County's Change Management Policies.
- 3.1.9** Business Application Software shall not require the creation, update, or deletion of any files on the database server outside the constructs of the database engine.
- 3.1.10** Business Application Software shall not create new databases or persistent database objects as part of its operation.
- 3.1.11** Business Application Vendor shall support application database backups/restores using Orange County's Enterprise Backup Tool. Currently, Orange County standard is CommVault's Galaxy iData-Agent for SQL Server.
- 3.1.12** Business Application Software shall provide an audit mechanism to record the date, time, and user id that last modified a given row in an application table.
- 3.1.13** Business Application Software shall utilize database referential integrity to eliminate the possibility of orphaned data.

4.0 Guidelines

- 4.1** These standards, polices, and guidelines shall be followed.

5.0 Enforcement

- 5.1** Exceptions to the guidelines shall be considered if overriding justification is provided. Upon Orange County's considerations of the overriding rationale, exceptions may be approved and a waiver may be granted.

ENTERPRISE SECURITY STANDARDS, POLICIES, AND GUIDELINES

WEB SECURITY STANDARD

1.0 Purpose

The purpose of this document is to establish requirements that will better manage and secure all web server platforms within the Orange County Government Board of County Commissioners (OCGBCC). Please refer to attachments entitled Web Security Standard and Anti-Virus Document.

2.0 Scope

The scope of this document applies to all web server platforms located within the OCGBCC.

3.0 Policies

3.1 Activity

Any and all web server installations, removals or modifications shall require the direct involvement and documented approval by the Information Systems and Service Enterprise Security unit (ISS-ESU).

3.2 Hardware

3.2.1 All hardware platforms operating as a web server shall abide by all standards, policies and guidelines of the OCGBCC Enterprise Systems unit.

3.2.2 All hardware platforms operating as a web server shall reside on server hardware. Any exception shall require a documented waiver by the Information Systems and Services Enterprise Security unit (ISS-ESU).

3.3 Software

3.3.1 Web Server Platforms

3.3.1.1 Microsoft

Microsoft's Internet Information Server (IIS) is the approved, supported web server platform for OCGBCC.

3.3.1.2 Apache Software Foundation

Apache Software Foundation's HTTP Server (Apache) is approved but is unsupported. Any production use of (Apache) shall include an appropriate support model that is approved by the ISS-ESU.

3.3.1.3 Other

Other web server platforms may qualify for use, but shall require an evaluation, approval and a documented waiver by the ISS-ESU.

3.3.2 Databases

3.3.2.1 Location

A database server shall not reside on the same hardware platform as a web server.

3.4 Security

3.4.1 General

All web servers shall comply with all other documented ISS-ESU standards to include, but not limited to: virus, patch and account management.

3.4.2 Account Management

3.4.2.1 Local Account Access

Only accounts with local administrator privileges shall be allowed to log on locally to a web server.

3.4.2.2 Process/Application Accounts

All web server processes and applications shall run only under a low privilege local account. Web server processes shall not run under an account with domain, power user or a local administrator privileges.

3.4.2.3 Web Server Anonymous Accounts

Web server anonymous accounts shall only have read and execute permissions to folders/files within the web server directories. Change and delete permissions to folders/files that are directly accessible via a web browser shall not be granted to web server anonymous accounts.

3.4.3 Permissions

3.4.3.1 Operating System Permissions

ISS-ESU shall secure the operating system's file/folder permissions and security policies of all web servers. These permissions are to be modified solely by ISS-ESU.

3.4.3.2 Vendor/Third Party Access

Local administrator privileges on web servers are for authorized personnel only. Access to vendors and any other third party shall be provided solely on a temporarily, case-by-case basis through ISS-ESU.

3.4.4 Java Server Engines

Java server engines are approved but are not supported. Any production use of a Java server engine shall include an appropriate support model that is approved by (ISS-ESU).

3.4.5 FTP

Web servers that also run an FTP server shall not map FTP directories to directories accessible via a web browser.

3.4.6 Other

- Shares are not allowed on any directory accessible via web browser.
- Microsoft Windows web servers and any web application shall not be installed on the same drive as the host operating system.
- Developer access to web server content directories shall be available by WebDav or FrontPage server extensions only.

4.0 Guidelines

- It is recommended that all web applications use the enterprise FTP and SMTP servers for all FTP/SMTP traffic.

5.0 Enforcement

Any web server not meeting the above criteria may be immediately disconnected from the OCGBCC network. Any employee found to have violated these policies may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term

Definition

FTP

File Transfer Protocol – The protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server.

WebDav

Web-based Distributed Authoring and Versioning – Extensions to HTTP that allows users to collaboratively edit and manage files on remote Web servers.

Front Page Extensions

A series of scripts that can be employed using Microsoft FrontPage, a visual HTML editor.

SMTP

Simple Mail Transfer Protocol – A protocol for sending e-mail messages between servers. In addition, SMTP is generally used to send messages from a mail client to a mail server.

ENTERPRISE SECURITY STANDARDS, POLICIES, AND GUIDELINES

DMZ SECURITY STANDARD

1.0 Purpose

The purpose of this document is to establish requirements that will better manage and secure all platforms within the Orange County Government Board of County Commissioners (OCGBCC). The DMZ is a secure environment with limited access to the OCGBCC internal network. Please refer to attachment entitled DMZ Security Standard.

2.0 Scope

The scope of this document applies to all platforms located within the OCGBCC DMZ.

3.0 Policies

3.1 Activity

Any and all activity within and through the OCGBCC DMZ shall require direct involvement and documented approval by the Information Systems and Service Enterprise Security unit (ISS-ESU).

3.2 Web Servers

All internal ISS-ESU policies apply to the OCGBCC DMZ and are augmented by the DMZ Security Standard. The following differences are noted:

- 3.2.1** Microsoft Internet Information Server (IIS) version 5.0 or higher shall be the only platform within the OCGBCC DMZ to run as a Web or FTP server.
- 3.2.2** All platforms within the OCGBCC DMZ shall be patched immediately upon the release and testing by the ISS-ESU.

3.3 Administrative Rights

ISS-ESU shall be the only group with administrative rights to servers in the DMZ.

3.4 Production Servers

The OCGBCC DMZ shall host production servers only.

3.5 Remote Access

Remote Access to the OCGBCC DMZ shall be allowed only using Microsoft Terminal Services or Microsoft Remote Desktop protocols.

3.6 Traffic

3.6.1 Internet Activity

HTTP/HTTPS/FTP/SMTP/IMAPS are the only protocols allowed from the Internet into the DMZ.

3.6.2 Internal Activity

Traffic using the following protocols from the DMZ to the internal network shall not be allowed: Kerberos, NetBIOS, Microsoft-DS, Microsoft's Well Known Ports (88, 135, 137, 138, 139, 389, 445, 464, 530, 543, 544, 636, 749, 3389), LDAP, RPC, SMB, RDP, HTTP, HTTPS, DNS, JOLT.

3.6.3 Routing

- 3.6.3.1** All approved access from the DMZ to the internal network shall be routed through a proxy server residing in the DMZ.
- 3.6.3.2** The Enterprise DMZ proxy server shall only use firewall conduits to access approved resources within the OCGBCC network.

3.7 Data

- 3.7.1** Any data accessible within the OCGBCC DMZ or directly accessible from it should be encrypted.
- 3.7.2** Any data accessible within the OCGBCC DMZ or directly accessible from it meeting the following criteria shall be encrypted: Name, addresses, phone numbers, email addresses, birthdates, federal/state/local document numbers, account numbers, race or religious information, employee identification numbers and all HIPAA information.
- 3.7.3** The OCGBCC DMZ shall not have access to data containing bank information.
- 3.7.4** The OCGBCC DMZ shall not have access to social security information.
- 3.7.5** The OCGBCC DMZ shall have read only access to live data, if such data is also used by applications residing in the internal OCGBCC network.

4.0 Guidelines

- Should databases in policy 3.7.4 need to receive updates by the OCGBCC DMZ, the write operations should be made to a physically separate “staging” data repository. This separate data repository should contain only updates for the specific records being changed. An application server within the internal network should be used to apply the changes in the staging data repository to the live database.
- The DMZ should access data repositories in the internal OCGBCC network using SQL database calls.

5.0 Enforcement

Any server found within the OCGBCC DMZ that does not meet the above criteria shall be immediately disconnected from the OCGBCC DMZ. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
Bank Information	Checking account numbers, credit card numbers, or any unique number from a bank institution.
HTTP	HyperText Transfer Protocol – The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.
HTTPS	HyperText Transfer Protocol over Secure Socket Layer (SSL) – By convention, URLs that require an SSL connection start with https: instead of just http:.
FTP	File Transfer Protocol – The protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server.
SMTP	Simple Mail Transfer Protocol – A protocol for sending e-mail messages between servers. In addition, SMTP is generally used to send messages from a mail client to a mail server.
IMAPS	Internet Message Access Protocol – A protocol for retrieving e-mail messages. With IMAP4, you can search through your e-mail messages for keywords while the messages are still on mail server and, then, choose which messages to download to your machine.
LDAP	Lightweight Directory Access Protocol – A set of protocols for accessing information directories.
DNS	Domain Name System (or Service or Server) – An Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on numeric IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.
SQL	Structured query language – SQL is a standardized query language for requesting information from a database.
DMZ	Demilitarized Zone – A computer term used for a protected network that sits between the Internet and the corporate network.
SSL	Secure Sockets Layer – A protocol for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.

ENTERPRISE SECURITY STANDARDS, POLICIES, AND GUIDELINES

ACCOUNT MANAGEMENT STANDARD

1.0 Purpose

The purpose of this document is to establish the rules for the creation, monitoring, management and removal of user accounts within the Orange County Government Board of County Commissioners (OCGBCC).

2.0 Scope

This document applies to all accounts provided for OCGBCC employees, consultants, temporary workers and all other affiliated third parties operating within OCGBCC information systems and networks.

3.0 Policies

3.1 Auditing

3.1.1 OCGBCC Employees

Users access accounts of all OCGBCC employees shall be compared daily to a list of employees that have had their employment terminated by OCGBCC.

3.1.2 Non-OCGBCC Employees

Users access accounts of all non-OCGBCC employees shall be compared on a quarterly basis to a list of all non-OCGBCC employees that have terminated their employment with the respective non-OCGBCC organization.

3.2 Account Creation

3.2.1 All user access accounts created shall have an associated OCGBCC service center request and approval from the appropriate authorized requestor.

3.2.2 All user access accounts shall be uniquely identifiable and associated with a private alpha/numeric password.

3.2.3 All user access accounts created for Non-OCGBCC employees shall have a specific, set expiration date.

3.3 Account Modification

3.3.1 Any account modifications shall come from, and be approved directly from, the individual's authorized requestor.

3.3.2 All authorized requestors shall, upon the change of an individual's role, responsibility or employment status, notify Information Systems Enterprise Security unit (ISS-ESU) via the OCGBCC service center.

3.3.3 All user access account modifications processed shall require the reconfirmation of all existing privileges before assigning the new, approved ones.

3.4 Account Removal

3.4.1 Inactive Accounts

Users access accounts not used within the last 45 days shall be disabled. Said accounts shall be deleted 45 days from their disabled date.

3.4.2 Terminated Employee Accounts

Users access accounts of employees, consultants, temporary workers and any other third parties (either OCGBCC or non-OCGBCC) whose employment has been terminated shall be immediately disabled. Said accounts shall be deleted 45 days from their disabled date.

3.5 Password Management

3.5.1 Password Responsibilities

All passwords shall be given directly to the owner only. Passwords are confidential information and shall not be disclosed to anyone but the owner. The password owner is directly responsible for the use of their password and shall not share or distribute it in any form.

3.5.2 General Password Requirements

Passwords shall conform to these specifications as a minimum.

3.5.2.1 Maximum password age: 45 days

3.5.2.2 Minimum password length: 6 characters

3.5.2.3 Account lockout threshold: 5 invalid logon attempts

3.5.3 Microsoft Windows Active Directory

All Microsoft Windows passwords shall be created in accordance with the following password rules:

3.5.3.1 Enforce password history: 6 passwords

3.5.3.2 Maximum password age: 45 days

3.5.3.3 Minimum password length: 6 characters

3.5.3.4 Account lockout duration: 3 minutes

3.5.3.5 Account lockout threshold: 5 invalid logon attempts

3.5.3.6 Reset account lockout counter: 3 minutes

3.6 Generic Accounts

3.6.1 All accounts are assigned to either individuals or applications. Generic accounts for use by multiple parties are prohibited. Any deviations from this policy require notification, documentation and approval by the ISS-ESU.

3.7 Account Management

3.7.1 ISS-ESU shall notify all authorized requestors on a quarterly basis of the need to comply with policy 2.3.2 of this document.

3.8 Application Accounts

3.8.1 All user application accounts should meet the Account Management Standard. Any deviations from this standard require notification, documentation and approval by the ISS-ESU.

3.8.2 Windows authentication should be used for application account authentication.

3.8.3 All system application accounts shall be assigned to their respective application, and not to a particular individual. Individuals shall not use a system application account.

4.0 Guidelines

- All user access accounts of individuals on extended leave (more than 30 days) should be disabled.
- All new user access accounts that have not been accessed within 30 days of creation should be disabled.

5.0 Enforcement

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension.

6.0 Definitions

Term	Definition
User access account	Any operating system, remote access or network account.
User application account	Any account associated with a specific application.
System application account	Any system account associated or required for an application.

ENTERPRISE SECURITY STANDARDS, POLICIES, AND GUIDELINES

ENCRYPTION AND CERTIFICATION AUTHORITIES

1.0 Purpose

The purpose of this document is to ensure that all Orange County Government Board of County Commissioner's (OCGBCC) sensitive data is secured by using strong encryption algorithms that have received substantial public review and have been proven to work effectively. Orange County Information Systems and Services Enterprise Security unit (ISS-ESU) provides access to a variety of Encryption Services and Enterprise Certification Authorities (CA). Please refer to attachment entitled Encryption Certification Document.

2.0 Scope

This document applies to all data transmitted and stored within the OCGGCC information systems. It applies to all OCGGCC employees, consultants, and all other affiliated third parties operating within the OCGGCC information systems and networks.

3.0 Policies

3.1 Activity

- 3.1.1** Any and all activity within and through the OCGGCC information systems involving encryption shall require direct involvement and documented approval by the Information Systems and Service Enterprise Security unit (ISS-ESU).
- 3.1.2** The ISS-ESU shall approve the storage and transfer of any data containing personal information and/or residing in the DMZ.

3.2 Encryption Algorithms

- 3.2.1** One of the following standard encryption ciphers shall be used to encrypt data. The key length for these algorithms shall be no less than 128bits:
 - Triple-DES (3DES)
 - Rijndael (AES)
 - RSA
 - Blowfish
 - Twofish
 - CAST
- 3.2.2** PGP is an approved encryption standard provided that the PGP private key used to encrypt and /or sign data has been generated using a cipher meeting the requirements in section 3.2.1.

3.3 Data Hashing

The following standard data hashing algorithms shall be used to hash data. The key length for the algorithms shall be no less than 128bits.

- MD5
- SHA-1
- SHA-2

3.4 SSL Certificates

Web Server, SSH, IMAPS, SMTPS SSL certificates should have key lengths of no less than 128bits.

3.5 Sensitive Data

Any data containing sensitive information, including, but not limited to: name, addresses, phone numbers, email addresses, birthdates, federal/state/local document numbers, account numbers, race or religious information, employee identification numbers and all HIPAA information, should be encrypted when stored and during network transfers.

3.6 DMZ

- 3.6.1** Any and all activity within and through the OCGGCC DMZ shall require direct involvement and documented approval by the Information Systems and Service Enterprise Security unit (ISS-ESU).
- 3.6.2** Any data accessible within the OCGGCC DMZ or directly accessible from it should be encrypted.
- 3.6.3** Any data accessible within the OCGGCC DMZ or directly accessible from it meeting the following criteria shall be encrypted: name, addresses, phone numbers, email addresses, birthdates, federal/state/local document numbers, account numbers, race or religious information, employee identification numbers and all HIPAA information.

3.7 Data Backups

- 3.7.1** Any backup of OCGBCC should be encrypted. Sensitive data as listed in 3.5 of this document shall be backed up using encryption algorithm standards found in 3.2.

3.8 Laptops and Removal Devices

- 3.8.1** All laptop hard drives should be encrypted.
- 3.8.2** Any sensitive data (see section 3.5 of this document) stored on laptops and removable devices shall be encrypted.
- 3.8.3** All individuals who work with sensitive data (see section 3.5 of this document) shall have their laptop hard drives encrypted.

4.0 Guidelines

- SSL certificates issued to servers and applications used by internet users should be provided by commercial CA authorities (i.e. Verisign, Thawte) to avoid security warnings from being presented to the end users.
- SSL certificates issued to servers and applications used by internal OCGBCC resources should be issued by OCGBCC's Certification Authority.

5.0 Enforcement

Any employee found to have violated these policies may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
Encryption	Transforming understandable data into a form that is incomprehensible and that looks like random noise.
Hashing	An algorithm that takes an entire message and, through process of shuffling, manipulating, and processing the bytes using logical operations, generates a small message digest of the data.
DMZ	De-Militarized Zone – A computer term used for a protected network that sits between the Internet and the corporate network.
Certification Authority (CA)	In cryptography, a certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties.