भारतसरकार रक्षामंत्रालय
Government of India Ministry of Defence
रक्षालेखामहानियंत्रक
Controller General of Defence Accounts
उलानबटाररोड़, पालम, दिल्लीछावनी-110010
Ulan Batar Road, Palam, Delhi Cantt – 110010
Ph- 011-25665863,25665763, Fax- 011-25675030
Email: cgdanewdelhi@nic.in

(IT&S Wing)

(Through Website only)

Mech/IT&S/159/Misc Corr   Dated: 14.12.2018

To

All PCsDA/CsDA

Subject: Information Security Policy

Reference: Hqrs. Office letter no. Mech/EDP/598/ORS/Vol-VI dt
          11.06.2015.

*****

    Please refer to the letter cited under reference. You are requested to find

enclosed Security Policy Version 1.0 and ensure compliance of all the security

provisions in all your offices.

    This issues with the approval of Jt.CGDA (IT&S)

(Amit Kumar)
ACGDA (IT&S)

Copy to:

IT&S (Local)   : For uploading on website.

— sd —
(Amit Kumar)
ACGDA (IT&S)

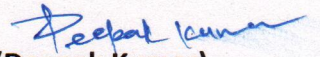| No. Mech/EDP/598/ORS/Vol-VI	Dated 11-6-2015

To,

    All PCsDA/CsDA

Sub: **Information Security Policy**

    Please find enclosed Information Security Policy version 1.0. This policy is framework for ensuring confidentiality, integrity and availability of information across the various offices and is comprehensive policy covering all aspects relating to password security policy, database credentials policy, server security policy, e-mail policy, remote access policy, data transmission policy etc.
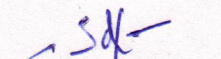
2.   It is requested to ensure that instructions contained in Information Security Policy should be complied with and necessary action may be taken in this regard strictly in PAOs offices under your jurisdiction.

    Jt. CGDA(IT) has approved.

(Deepak Kumar)
Sr. ACGDA (IT)

Copy to :-

1. The CDA   :   For information w.r.t. your letter no. IT&SD/Sys/
   O/o the IT & SDC   Misc dated 06-01-2015 & no. System/ IS Audit/Vol-
   Secunderabad.   I dated 14-05-2015.

2. EDP (Local)   :   For uploading on website.

(Deepak Kumar)
Sr. ACGDA (IT)

Information Security Policy

Version: 1.0

Controller General of Defence Accounts
New Delhi

Table of Contents

Introduction

*It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public – **Clay Shirky***

We are living in a digital age. All of our business processes are increasingly becoming computerised. While technology enables us to process vast amounts of data with speed and accuracy to provide instant quality service to our clients, it also has an unintended side effect. The same technology also enables the bad guys to easily steal the identities of individuals and sensitive information. The bad guys do not even have to visit the locations where the information is stored; they can do it sitting in a remote location, even in a different country.

This Information Security Policy is an attempt to create a framework for ensuring confidentiality, integrity and availability of information across the Defence Accounts Department. However, security is not a one shot process where we define the policy, the procedures to implement it and the audit to establish the policy compliance. Security is a continuous process in any organisation with people getting transferred out, retirements, new people coming in, improvements in technology and the memories of existing people fading out. People are said to be the weakest link in the security chain. Any policy that does not take this fact into account is bound to fail. Each person in the Department has a role to play in ensuring this policy gets implemented to yield the desired results.

Information Technology is a fast moving field. Some parts of this policy will eventually get outdated and need to be replaced with more relevant parts. This policy will be reviewed at least once every two years to keep it up-to-date.

Chapter 1   Password Construction Guidelines

1.1 Overview
Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network. This guideline provides best practices for creating secure passwords.

1.2 Purpose
The purpose of this guidelines is to provide best practices for the creation of strong passwords.

1.3 Scope
This guideline applies to employees, contractors, consultants, temporary and other workers. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

1.4 Guidelines
All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:
· Contain at least 12 alphanumeric characters.
· Contain both upper and lower case letters.
· Contain at least one number (for example, 0-9).
· Contain at least one special character (for example,!$%^&*()_+|~-=\`{} []:";'<>?,/).

Poor, or weak, passwords have the following characteristics:
· Contain less than eight characters.
· Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
· Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
· Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
· Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
· Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
· Are some version of "Welcome123" "Password123" "Changeme123"

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To

Remember" could become the password TmB1w2R! or another variation. (NOTE: Do not use either of these examples as passwords!)

Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

Chapter 2   Password Protection Policy

2.1 Overview
Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of resources. All users, including contractors and vendors with access to the Department's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.2 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.3 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any office, has access to the Department's network, or stores any non-public information of the Department.

2.4 Policy

i) Password Creation
    a) All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
    b) Users must not use the same password for official accounts as for personal accounts.
    c) Where possible, users must not use the same password for various access needs.
    d) User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

ii) Password Change
    a) All system-level passwords must be changed on at least a quarterly basis.
    b) All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
    c) Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

iii) Password Protection
    a) Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
    b) Passwords must not be inserted into email messages or other forms of electronic communication.

c) Passwords must not be revealed over the phone to anyone.
d) Do not reveal a password on questionnaires or security forms.
e) Do not hint at the format of a password (for example, "my family name").
f) Do not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
g) Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
h) Do not use the "Remember Password" feature of applications (for example, web browsers).
i) Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

iv) Application Development
Application developers must ensure that their programs contain the following security precautions:
a) Applications must support authentication of individual users, not groups.
b) Applications must not store passwords in clear text or in any easily reversible form.
c) Applications must not transmit passwords in clear text over the network.
d) Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

v) Use of Passwords and Passphrases
Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters.
An example of a good passphrase:
"The*?#>*@TrafficOnThe101Was*&#!#ThisMornin
g"
All of the rules above that apply to passwords apply to passphrases.

Chapter 3   Email Policy

3.1 Overview
Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

3.2 Purpose
The purpose of this email policy is to ensure the proper use of the Department's email system and make users aware of what is acceptable and unacceptable use of the email system. This policy outlines the minimum requirements for use of email within the Departmental Network.

3.3 Scope
This policy covers appropriate use of any email sent from a Departmental email address and applies to all employees, vendors, and agents operating on behalf of the Department.

3.4   Policy
a) All use of email must be consistent with policies and procedures of ethical conduct, safety, compliance with applicable laws and proper official practices.
b) Email account should be used primarily for office related purposes; personal communication is permitted on a limited basis.
c) All data contained within an email message or an attachment must be secured according to the *Data Protection Standard*.
d) Email that is identified as a official record shall be retained according to the Record Retention Schedule.
e) The email system shall not to be used for the creation or distribution of any disruptive or offensive messages. Employees who receive any emails with this content from any employee should report the matter to their supervisor immediately.
f) Users are prohibited from automatically forwarding the Departmental email to a third party email system. Individual messages which are forwarded by the user must not contain confidential information.
g) Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct official business, to create or memorialize any binding transactions, or to store or retain email on behalf of the Department. Using a reasonable amount of resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a is prohibited.

Chapter 4 Clean Desk Policy

4.1 Overview
A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

4.2 Purpose
The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information is secure in locked areas.

4.3 Scope
This policy applies to all employees and affiliates.

4.4 Policy
   a) Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
   b) Computer workstations must be locked when workspace is unoccupied.
   c) Computer workstations must be shut completely down at the end of the work day.
   d) Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
   e) File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
   f) Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
   g) Laptops must be either locked with a locking cable or locked away in a drawer.
   h) Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
   i) Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
   j) Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
   k) Whiteboards containing Restricted and/or Sensitive information should be erased.
   l) Lock away portable computing devices such as laptops and tablets.
   m) Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
   n) All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Chapter 5   **Workstation Policy**

5.1   Overview
See Purpose.

5.2   Purpose
The purpose of this policy is to provide guidance for workstation security in order to ensure the security of information on the workstation and information the workstation may have access to.

5.3 Scope
This policy applies to all employees, clients and contractors with a personal-workstation connected to the Departmental network.

5.4 Policy
Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, and that access to sensitive information is restricted to authorized users.

The Department will implement physical and technical safeguards for all workstations that access electronic information to restrict access to authorized users.

Appropriate measures include:
   a) Restricting physical access to workstations to only authorized personnel.
   b) Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
   c) Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with the *Password Policy*.
   d) Ensuring workstations are used for authorized purposes only.
   e) Never installing unauthorized software on workstations.
   f)   Storing all sensitive information on network servers
   g) Keeping food and drink away from workstations in order to avoid accidental spills.
   h) Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
   i)   Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
   j)   Exit running applications and close open documents
   k) Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
   l)   If wireless network access is used, ensure access is secure by following the *Wireless Communication policy*

Chapter 6   Digital Signature Policy

6.1   Overview
See Purpose.

6.2   Purpose
The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

6.3 Scope
This policy applies to all employees, contractors, and others dealing with a Department provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non-Departmental affiliated persons or organizations.

6.4 Policy
A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

I) Responsibilities
Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

ii) Signer Responsibilities
   a) Signers must obtain a signing key pair from the Department's Identity Management Group. This key pair will be generated using the Department's Public Key Infrastructure (PKI) and the public key will be signed by the Department's Certificate Authority (CA).
   b) Signers must sign documents and correspondence using software approved by the IT wing.
   c) Signers must protect their private key and keep it secret.
   d) If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact Identity Management Group immediately to have the signer's digital key pair revoked.

Iii) Recipient Responsibilities
   a) Recipients must read documents and correspondence using software approved by IT wing.

b) Recipients must verify that the signer's public key was signed by the Department's Certificate Authority (CA), by viewing the details about the signed key using the software they are using to read the document or correspondence.

c) If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.

d) If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to the Identity Management Group.

Chapter 7   Acceptable Use Policy

7.1 Overview
Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

7.2 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment at the office. Inappropriate use exposes the Department to risks including virus attacks, compromise of network systems and services, and legal issues.

7.3 Scope
This policy applies to the use of information, electronic and computing devices, and network resources to conduct official business.. All employees, contractors, consultants, and temporary workers are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the Departmental policies and standards, and local laws and regulation.

7.4   Policy

i) General Use and Ownership
   a) You have a responsibility to promptly report the theft, loss or unauthorized disclosure of confidential information.
   b) You may access, use or share confidential information only to the extent it is authorized and necessary to fulfill your assigned job duties.
   c) For security and network maintenance purposes, authorized individuals may monitor equipment, systems and network traffic at any time.
   d) The InfoSec team may audit networks and systems on a periodic basis to ensure compliance with this policy.

ii) Security and Confidential Information
   a) Providing access to another individual who is not authorized, either deliberately or through failure to secure its access, is prohibited.
   b) All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
   c) The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
   d) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

ii) Unacceptable Use

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Unauthorized copying of copyrighted material .
2. Accessing data, a server or an account for any purpose other than conducting official business, even if you have authorized access, is prohibited.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
6. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
7. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
8. Circumventing user authentication or security of any host, network or account.
9. Introducing honeypots, honeynets, or similar technology on the network.
10. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
11. Unauthorized use, or forging, of email header information.
12. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Chapter 8　　**Server Security Policy**

8.1 Overview
Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

8.2 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment. Effective implementation of this policy will minimize unauthorized access to confidential information.

8.3 Scope
All employees, contractors, consultants, temporary and other workersmust adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by the Department.

8.4 Policy

i) General Requirements
All internal servers deployed must be owned by an operational group that is responsible for system administration. Approved (by InfoSec) server configuration guides must be established and maintained by each operational group. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec.
The following items must be met:
  a) Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  b) Server contact(s) and location, and a backup contact
  c) Hardware and Operating System/Version
  d) Main functions and applications, if applicable
  e) Configuration changes for production servers must follow the appropriate change management procedures
  f) For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

ii) Configuration Requirements
  a) Operating System configuration should be in accordance with approved InfoSec guidelines.
  b) Services and applications that will not be used must be disabled where practical.
  c) Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
  d) The most recent security patches must be installed on the system as soon as

practical, the only exception being when immediate application would interfere with business requirements.

e) Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

f) Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

g) If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

h) Servers should be physically located in an access-controlled environment.

i) Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Iii) Monitoring

a) All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

b) All security related logs will be kept online for a minimum of 1 week.

c) Daily incremental backups will be retained for at least 1 month.

d) Weekly full backups of logs will be retained for at least 1 month.

e) Monthly full backups will be retained for a minimum of 2 years.

f) Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

Chapter 9   **Database Credentials Policy**

9.1 Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

9.2 Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on the Departmental networks.

Software applications running on the networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

9.3 Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on theDepartmental Network. This policy applies to all software (programs, modules, libraries or APIS) that will access a , multi-user production database. It is recommended that similar requirements be in place for non-production servers and lab environments since they don't always use sanitized information.

9.4 Policy

In order to maintain the security of internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

i) Storage of Data Base User Names and Passwords
  a) Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
  b) Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
  c) Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
  d) Database credentials may not reside in the documents tree of a web server.

e) Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

ii) Retrieval of Database User Names and Passwords
a) If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
b) The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
c) For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

Iii) Access to Database User Names and Passwords
a) Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
b) Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
c) Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Chapter 10   **Information Logging Standard**

10.1 Overview
Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

10.2 Purpose
The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

10.3 Scope
This policy applies to all production systems on the Departmental Network.

10.4 Standard

i) General Requirements
All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:
   a) What activity was performed?
   b) Who or what performed the activity, including where or on what system the activity was performed from (subject)?
   c) What the activity was performed on (object)?
   d) When was the activity performed?
   e) What tool(s) was the activity was performed with?
   f) What was the status (such as success vs. failure), outcome, or result of the activity?

ii) Activities to be Logged
Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:
   a) Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
   b) Create, update, or delete information not covered in #1;
        1. Initiate a network connection;
        2. Accept a network connection;
   c) User authentication and authorization for activities covered in #1 or #2 such as user login and logout;
        d) Grant, modify, or revoke access rights, including adding a new user or

        group, changing user privilege levels, changing file permissions, changing

database object permissions, changing firewall rules, and user password changes;

e) System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;

f) Application process startup, shutdown, or restart;

g) Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and

h) Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

iii) Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

a) Type of action – examples include authorize, create, read, update, delete, and accept network connection.

b) Subsystem performing the action – examples include process or transaction name, process or transaction identifier.

c) Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.

d) Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.

e) Before and after values when action involves updating a data element, if feasible.

f) Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.

g) Whether the action was allowed or denied by access-control mechanisms.

h) Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

iv) Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

a) Logs in a well-documented format sent via *syslog*, *syslog-ng*, or *syslog-reliable* network protocols to a centralized log management system;

b) Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and

c) Other open logging mechanisms supporting the above requirements 18

Chapter 11 **Router and Switch Policy**

11.1 Overview
See Purpose.

11.2 Purpose
This document describes a required minimal security configuration for all routers and switches connecting to a production network

11.3 Scope
All employees, contractors, consultants, temporary and other workers must adhere to this policy. All routers and switches connected to the production networks are affected.

11.4 Policy
Every router must meet the following configuration standards:

a) The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.

b) The following services or features must be disabled:
   1. IP directed broadcasts
   2. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
   3. TCP small services
   4. UDP small services
   5. All source routing and switching
   6. All web services running on router
   7. Telnet, FTP, and HTTP services
   8. Auto-configuration

c) All routing updates shall be done using secure routing updates.

d) SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

e) Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

Chapter 12 Wireless Communication Standard

12.1 Overview
See Purpose.

12.2 Purpose
This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Departmental network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Team are approved for connectivity..

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Security (Infosec) approved support organization.

12.3 Scope
All employees, contractors, consultants, temporary and other workers including all personnel that maintain a wireless infrastructure device on behalf of the Department must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

Infosec must approve exceptions to this standard in advance.

12.4 Standard

i) General Requirements
All wireless infrastructure devices that connect to the Departmental network must:
   a) Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
   b) Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
   c) All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

ii) Lab and Isolated Wireless Device Requirements
   a) Lab device Service Set Identifier (SSID) must be different from a production device SSID.
   b) Broadcast of lab device SSID must be disabled.

Chapter 13   Wireless Communication Policy

13.1 Overview
With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

13.2 Purpose
The purpose of this policy is to secure and protect the information assets. This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the Departmental network .

13.3 Scope
All employees, contractors, consultants, temporary and other workers at including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the Department must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to the Departmental network or reside on a Departmental site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

13.4 Policy

All wireless infrastructure devices must:
   a) Abide by the standards specified in the Wireless Communication Standard.
   b) Be installed, supported, and maintained by an approved support team.
   c) Use approved authentication protocols and infrastructure.
   d) Use approved encryption protocols.
   e) Maintain a hardware address (MAC address) that can be registered and tracked.
      .

Chapter 14   Remote Access Policy

14.1 Overview
See Purpose.

14.2 Purpose
The purpose of this policy is to define standards for connecting to the Department's network from any host. These standards are designed to minimize the potential exposure to damages which may result from unauthorized use of Departmental resources. Damages include the loss of sensitive or confidential data, damage to public image, damage to critical internal systems, etc.

14.3 Scope
This policy applies to all employees, and contractors, with a computer or workstation used to connect to the Departmental network. This policy applies to remote access connections used to do work on behalf of the Department, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to DSL, VPN, SSH.

14.4 Policy
Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of the Departmental network:
  · *Acceptable Encryption Policy*
  · *Wireless Communications Policy*
  · *Acceptable Use Policy*

Requirements
   a) Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the *Password Policy*.
   b) At no time should any employee provide their login or email password to anyone, not even family members.
   c) Employees and contractors with remote access privileges must ensure that their personal computer or workstation, which is remotely connected to Departmental network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
   d) Non-standard hardware configurations must be approved by InfoSec for access to the Departmental network.
   e) All hosts that are connected to internal networks via remote access technologies must use the most up-to-date anti-virus software.

Chapter 15 **Bluetooth Policy**

15.1 Overview
 Bluetooth enabled devices are exploding on the Internet at an astonishing rate. At the range of connectivity has increased substantially. Insecure Bluetooth connections can introduce a number of potential serious security issues. Hence, there is a need for a minimum standard for connecting Bluetooth enable devices.

15.2 Purpose
The purpose of this policy is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the Departmental network. The intent of the minimum standard is to ensure sufficient protection to confidential data.

15.3 Scope
This policy applies to any Bluetooth enabled device that is connected to Departmental network or owned devices.

15.4 Policy

i) Version
No Bluetooth Device shall be deployed on the Departmental equipment that does not meet a minimum of Bluetooth v2.1 specifications without written authorization from the Infosec Team. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

ii) Pins and Pairing
When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where you PIN can be compromised. If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, you must refuse the pairing request and report it to Infosec, through your Help Desk, immediately.

Iii) Device Security Settings
  a) All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
  b) Use a minimum PIN length of 8. A longer PIN provides more security.
  c) Switch the Bluetooth device to use the hidden mode (non-discoverable)
  d) Activate Bluetooth only when it is needed.
  e) Ensure device firmware is up-to-date.

iv) Security Audits
The Infosec Team may perform random audits to ensure compliancy with this policy. In the process of performing such audits, Infosec Team members shall not eavesdrop on any phone conversation.

v) Unauthorized Use
The following is a list of unauthorized uses of Bluetooth devices:

a) Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
b) Unauthorized modification of Bluetooth devices for any purpose.

vi) User Responsibilities
a) It is the Bluetooth user's responsibility to comply with this policy.
b) Bluetooth mode must be turned off when not in use.
c) Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.
d) Bluetooth users must only access information systems using approved Bluetooth device hardware, software, solutions, and connections.
e) Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
f) Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
g) Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to Infosec.

Chapter 16 **Application Security Policy**

16.1 Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be plugged prior to production deployment.

16.2 Purpose

The purpose of this policy is to define web application security assessments. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of services available.

16.3 Scope

All web application security assessments will be performed by delegated security personnel either employed or contracted . All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of the Department is strictly prohibited.

16.4 Policy

i) Criteria

Web applications are subject to security assessments based on the following criteria:

  a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
  b) Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
  c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
  d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
  e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

ii) Risk Mitigation

All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the Open Web Application Security Project (**OWASP**) Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

  a) High – Any high risk issue must be fixed immediately or other mitigation

strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

b) Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

c) Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

Iii) Security Assessment Levels

The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

a) Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

b) Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

c) Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

Chapter 17   Equipment Disposal Policy

17.1 Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of data, some of which is considered sensitive. In order to protect our data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

17.2 Purpose

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by the Department.

17.3 Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed , including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All employees and affiliates must comply with this policy.

17.4 Policy

a) When Technology assets have reached the end of their useful life they should be properly disposed by an Equipment Disposal Team.

b) The Equipment Disposal Team will securely erase all storage mediums in accordance with current industry best practices.

c) All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks.

d) All electronic drives must be degaussed or overwritten with a disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

e) The Equipment Disposal Team will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

f) Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed   .27

Chapter 18 Acceptable Encryption Policy

18.1 Overview
See Purpose.

18.2 Purpose
The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

18.3 Scope
This policy applies to all employees and affiliates.

18.4 Policy

i) Algorithm Requirements
    a) The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.
    b) The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.
    c) Signature Algorithms

Algorithm	Minimum Key Length
ECDSA	P-256
RSA	2048
LDWM	SHA256

ii) Key Agreement and Authentication
    a) Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
    b) End points must be authenticated prior to the exchange or derivation of session keys.
    c) Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
    d) All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
    e) All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

Iii) Key Generation
    a) Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
    b) Key generation must be seeded from an industry standard random number 28

generator (RNG).

Chapter 19   Disaster Recovery Plan

19.1 Overview
Since disasters happen so rarely, management often ignores the disaster recovery planning process. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

19.2 Purpose
This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

19.3 Scope
This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

19.4 Policy
The following contingency plans must becreated:
   a) Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
   b) Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
   c) Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
   d) Criticality of Service List: List all the services provided and their order of importance.
   e) It also explains the order of recovery in both short-term and long-term timeframes.
   f) Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences. The plan, at a minimum, should be reviewed an updated on an annual basis.

Chapter 20 **Human Resource Policy**

20.1 Overview
Humans are the weakest link in the entire information security chain. Unless everyone involved does her/his bit, the security policy will not yield the desired results.

20.2 Purpose
The policy briefly outlines the roles of various categories of personnel.

20.3 Scope
The policy is directed at all the stakeholders.

20.4 Policy
a) The management must commit the resources necessary to implement the security policy.
b) The in-house software development teams must be trained in the best practices of development and secure coding techniques.
c) System administrators must be trained to have adequate knowledge to manage the IT infrastructure under their control.
d) End users must be aware of the security policy of the Department and play their role in complying with it.

Data Transmission Policy

21.1 **Overview**

Malicious users may intercept or monitor plaintext data transmitting across unencrypted network and gain unauthorized access to the sensitive data. Therefore, anyone moving sensitive data through a network must use secure, authenticated, and industry-accepted encryption mechanisms.

Sensitive data must be encrypted when transmitted across networks to protect against eavesdropping of network traffic by unauthorized users. In cases where source and target endpoint devices are within the same protected subnet, sensitive data transmission must still be encrypted as recommended below due to the potential for high negative impact of a covered data breach. The types of transmission may include client-to-server, server-to-server communication, as well as any data transfer between core systems and third party systems.

21.2 **Scope**

This policy applies to all software developers, employees and affiliates.

21.3 **Policy**

a) Where the covered device is reachable via web interface, web traffic must be transmitted over Secure Sockets Layer (SSL), using only strong security protocols, such as Transport Layer Security (TLS).

b) Email is not considered secure and must not be used to transmit covered data unless additional email encryption tools are used. Sensitive data transmitted over e-mail must be secured using cryptographically strong e-mail encryption tools such as PGP or S/MIME. Alternatively, prior to sending the e-mail, user should encrypt covered data using compliant File Encryption tools and attach the encrypted file to e-mail for transmission.

c) Non-web transmission of sensitive data should be encrypted via application level encryption.

d) Where the application database resides outside of the application server, the connection between the database and application should also be encrypted using FIPS compliant cryptographic algorithms.

e) Where application level encryption is not available for non-web covered data traffic, implement network level encryption such as IPSec or SSH tunneling.

f) In general, encryption should be applied when transmitting sensitive data between devices in protected subnets with strong firewall controls.

g) When the software is getting developed the developers will be made aware of the security policy so that the policy requirements are built into the software right from the beginning.

h) Examples of insecure network protocols and their secure alternatives include:

Protocol	Unsafe	Safe
Web Access	HTTP	HTTPS
File transfer	FTP, RCP	FTPS,SFTP,SCP
Remote Shell	Telnet	SSH2 Terminal
Remote desktop	VNC	Radmin, RDP

Some Definitions

Availability
The information is available when needed..

Confidentiality
Ensuring only authorised entities can read the information.

Guideline
Recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place

InfoSec
Short hand for Information Security.

Integrity
Ensuring only authorised entities can modify the information.

Policy
It is a high level description of controls that must be in place to protect information. It also defines roles responsibilities and the scope of information to be protected.

Procedure
Specific step by step instructions to implement the policies, standards and guidelines.

Standard
Specific low level mandatory controls that help enforce and support the information security policy.