GUN CARRIAGE FACTORY
JABALPUR

ISMS

Information Security Process Management Manual

ISO/IEC 17799:2005(E) / ISO 27002

GUN CARRIAGE FACTORY, JABALPUR.

INFORMATION SECURITY PROCESS MANAGEMENT

1. PURPOSE:-

To carry out various Information Security Operations of Information Technology Centre of GCF, Jabalpur.

2. SCOPE:-

The following domains are applicable to the Information Security Processes of I.T. Centre.

1. Information security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

3. METHODOLOGY:-

All the domains mentioned above, relevant to IT Security, are analyzed and examined by the key personnel of IT Operations. After approval of the top management the same is implemented and managed by executing personnel.

3.1 ***Information security policy***

3.1.1 ***Information security policy document***

The information security policy approved by the management, published and communicated as appropriate to employees is as follows :-

Information Technology Centre (ITC) of Gun Carriage Factory, Jabalpur is committed to provide necessary information inputs to management for well informed decision making while ensuring at the same time, complete confidentiality, integrity and sanctity of available electronic data with adoption improvement and provision of selected information processing system.

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

Information security policy is reviewed at the end of every month in ITC Computerization meeting chaired by the General Manager. It will also be reviewed half yearly by OFB Kolkata and compliance report shall be submitted to OFB.

3.2 *Organization of information security*

3.2.1 Allocation of information security responsibilities

Information Security Officer is appointed by the General Manager and the name of the officer is communicated to Ordnance Factory Board, Kolkata. Duty allocation of the employees of ITC is documented and responsibilities communicated to individuals.

3.2.2 Authorization process for information processing facilities

Monthly computerization meeting is chaired by the GM, wherein purchase of IT equipment, local information processing facilities and their changes is authorized.

3.2.3 Independent review of information security

Independent review is being conducted by a team of internal auditors in every six months as approved by General Manager.

3.2.4 Addressing security in external party agreements

a) The service provider has to accept terms and condition as mentioned in service contract.
b) HDD (Storage Media) like items can not be taken out by the service provider.
c) A Non Disclosure Agreement has to be signed by the service provider as mentioned in stamp paper of value 100/- duly notarized or signed by the service provider in presence of Oath Commissioner.

3.3 *Asset management*

3.3.1 Inventory of assets

Inventory is maintained for H/W assets and for software their licenses and validity are maintained. Broadband connections and their technical details, rental bills are maintained by Engineering Office.

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

3.3.2 Ownership of assets

Ownership is addressed for H/W assets (Client PCs and Printers etc.). User shall sign the acceptance of the hardware. IT department is the owner of information processing assets, like servers. Labeling is done on each equipment by ITC for explicit identification.

3.3.3 Acceptable use of assets

A DOs and DONTs document for users/operaters is available which are circulated through office memos. A policy (IS Policy) is defined for verification of its implementation approved by General Manager.

3.3.4 Information classification

All the information assets are classified in terms of its value, legal requirements, sensitivity and criticality to the organization. On requisition basis information can be given after the authorization and records are maintained for the same. Red, Blue, Green, Yellow.

3.3.5 Information labeling and handling

Hardware is labeled with physical stock no and security classification

3.4 ***Human resource security***

3.4.1 Screening

Police verification and academic verification is done for employees and external users as per the govt. rule.

3.4.2 Roles and responsibilities

General roles and responsibilities of the employees and external users are communicated and got acknowledged during joining and periodic meeting. External users Records such as internet usage & E-proc. register is maintained.

3.4.3 Confidentiality agreements

General non-disclosure agreement is signed by regular employee and external user like COD, LAO and SQAE etc. during joining as per govt. norms.

3.4.4 Information security awareness, education and training

Security awareness training program is conducted by OFILs/In-house training cell, for the employees and external users in definite period concerning the issues like updates in policies

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

and procedures. A DOs and DONTs policy issued by OFB is circulated to each employee and external user.

3.4.5 Disciplinary process

There is a disciplinary policy for the employees and external users as per govt. rules. Failing which, a disciplinary action is being taken against the person.

3.4.6 Termination process

a) Employees and external users when terminated or transferred are removed from the user domain and denied the access of the system..
b) Employees and external users have to surrender all assets in terms of ITC No dues clearance, provided by the ITC before terminating to other organization/department.
c) Employees and external users will lose access right to the information and information processing facilities after termination or transfer i.e. login ids and privileges shall lapse, email ids are centrally managed by OFB.

3.5 Physical and environmental security 3.5.1 Physical security perimeter

The factory perimeter is secured through fencing. metal control entry gates, manned reception are there to check each and individual.

3.5.2 Physical entry controls

a) Entry control is at the main entrance. The main gate is manned by security personnel.
b) Entry control at ITC is performed through locks
c) Main server's room is accessible through Electronic Identity Access Lock.

3.5.3 Equipment placement and protection

a) There are fire extinguishers inside the IT department and data centre
b) IT department is equipped with fire alarm

3.5.4 Supporting utilities

Uninterruptible power supply (10KV x 2) is supplying power to servers and network devices without having any hazard. Air conditioning is being provided to each and every room.

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

3.5.5 Cabling security

The power and telecommunications cable, carrying data or supporting information services is protected by underground GI pipes.

3.5.6 Equipment maintenance

a) maintenance of all hardware like servers, desktops, network devices, printers are either under AMC or warranty.
b) Faults are logged through http://complaint.gcf done by respective suppliers/vendors authorized agents.
c) Service reports are maintained
d) Permission like gate pass is required for taking equipment out of the premises.

3.5.7 Secure disposal or re-use of equipment

a) All equipments are disposed as per the condemnation policy (7 Years)
b) Formal disposal procedure as per ministry guidelines MHA-OM no.14/2-99-T dated 22.6.2001 is followed for the HDD of the PCs
c) The other parts of the PC are disposed through normal procedure.
d) Equipments which are condemned as per procedure in vogue are not reused.

3.5.8 Removal of property

Equipment, information and software is not taken off-site without prior authorization.

3.6 Communications and operations management 3.6.1

Documented operating procedures

Operating procedures are documented, maintained and available to all users who need it and are also available online in the form of ISO 9000 documentation.

3.6.2 Change management

a) ISO procedure is followed to make changes in information processing facilities and system
b) Changes are approved before implementation and records are maintained.

3.6.3 Separation of development, test and operational facilities

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

Development and testing facilities are isolated from operational facilities

3.6.4 Third party service delivery

It is mentioned in all maintenance contracts.

3.6.5 Capacity management

The capacity demands are monitored and projections of future capacity requirements are made, to ensure that adequate bandwidth, processing power and storage are available in ITC.

3.6.6 System acceptance

a) Acceptance criteria for items are given by OFB.
b) Acceptance test carried out as per purchase specification. DGS & D inspection also taken into consideration.

3.6.7 Controls against malicious code

a) All workstations have antivirus software
b) No explicit virus problem is reported
c) Trend-Micro anti-virus is being updated centrally by OFB.
d) Internet is being provided to limited persons through a separate LAN.
e) All the machines have two accounts administrator's account and guest account.

3.6.8 Information backup

a) All the database & programs are backed up daily CD/DAT.
b) External hard disk drive is used for data backup residing on PC & users are themselves responsible for taking back up of their own data residing on such PCs.

3.6.9 Network controls

a) Firewall is fully under control of OFB.
b) The internet broadband connection is separated from factory LAN.

3.6.10 Disposal of media

Media containing information which are no longer required are disposed of securely and safely as per the guidelines of Mins. Of Home affair (Ref. SI no 29 of MHA-OM no. 14/2/99 –T dated 22.06.200 1)

3.6.11 Media in transit

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

No media is sent by post or courier outside of the factory.

3.6.12 Electronic messaging

The information involved in electronic messaging is well protected because no local email server present.

3.6.13 Publicly available information

a) The integrity of the publicly available information is ensured and protected by NIC mail server.
b) Contents are sent to OFB based on the pre-requisite set by the board. GM office takes care of the data to be published.

3.6.14 Audit logging

a) Audit logs are recorded involving user activities, exceptions and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring.
b) Logging facility and log information are well protected against tampering and unauthorized access.
c) Log activities are reviewed on event basis by the administrator

3.6.15 Clock syncronisation

System clocks of all information processing system within the organization or security domain is synchronized with an agreed accurate time source.

3.7 Access control

3.7.1 Access control policy

Access control policy is developed and reviewed based on the business and security requirement and is authorized by head of respective department such as privileges granted to users (eg. Add, delete, modify, cancel etc.)

3.7.2 User registration

User registration and deregistration procedure for granting or revoking access to all information system and services is done through office notes.

3.7.3 Privilege management

a) The allocation and use of privileges in information system environment is restricted and controlled i.e. , privileges are allocated on need to use basis.

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

b) Privileged accounts are not used for normal use like internet browsing, email etc.

3.7.4 User password management

a) Allocation and reallocation of passwords are controlled through a formal management process
b) Positive identification (e.g. verification of date of birth, mother's maiden name or any other registered personal information) is done before allocating password by telephone.
c) Mandatory change of password is enforced when an account is used first time after it is created or password is reset by administrator.

3.7.5 Review of user access right

There is a process to review user access right at regular intervals. Example Special privilege review every three months, normal privileges every six months.

3.7.6 Clear desk and clear screen policy

a) Clear desk policy for retention period and its disposal w.r.t papers and removable storage media is followed according to security guidelines of Govt. of India issued time to time.

b) Users are automatically logged off after a certain period of non-activity.

3.7.7 External connection control

External connection is not allowed in order to control access by remote users, only OFB have the remote access.

3.7.8 Segregation in networks

There are physically separate networks for internet access and factory LAN/OFB WAN access.

3.7.9 Secure log-on procedures

a) Access to operating system is controlled by secure log-on procedure.
b) Protocol centrally given by OFB is being used.

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

3.7.10 User identification and authentication

a) Group user IDs shall be used for those applications wherever applicable.

b) Unique user ID is provided to every user such as operators, system administrators and all other staff including technical.

c) Authentication technique is used to substantiate the claimed identity of user
d) Shared accounts are not used.

3.7.11 Password management system

Password management system enforces various password controls such as enforce periodic password changes, store passwords in encrypted form, not display passwords on screen, enforcing users to select strong passwords (password length, complexity), restricting reuse of passwords, enforcing account lockout in case of attempt to access wrong passwords.

3.7.12 Session time-out

Inactive session is terminated after a defined period of inactivity.

3.7.13 Information access restriction

a) Access to information and application system functions by users and support personnel is restricted in accordance with the defined access control policy (For example:- File access, data access, service access etc.) such role based access controls are implemented in the applications.
b) Z-drive is being used for sharing the information on LAN
c) Computing system of CDA (LAO) is isolated from factory LAN.

3.8 information systems acquisition, development and maintenance 3.8.1

Security requirement analysis specification

The enhanced system installed is password controlled both at user and administrative level. Physical entry is restricted in server room.

3.8.2 Validation checks

Validation checks (input data, output data, internal processing)have been incorporated in the applications to prevent errors, loss of integrity and misuse of information/data.

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

3.8.3 Control of operational software

Installation of software on operational systems are controlled through programmer login.

3.8.4 Access control to program source code

a) Program source libraries are controlled through programmer logins (PPC and Payroll).
b) Super user login is separated from programmer's login.

3.8.5 Change control procedures

Authorization of changes is done through office notes . this procedure addresses analysis of impact of changes, rollback procedure in case of unsuccessful changes etc.

3.8.6 Technical review of applications after operating system changes

a) Test of business and critical applications are done to study the adverse impact on organizational operations and security is being reviewed after change to operating system.
b) Operating system on the PC is connected to the internet is upgraded periodically i.e. to install service packs, patches, hot fixes etc.

3.8.7 Control of technical vulnerabilities

COMNET is not exposed to the internet as this system is prone to technical vulnerabilities.

3.9 Information security incident management

3.9.1 Reporting information security events, weaknesses

a) Information security events are reported through appropriate management channels as quickly as possible
b) Central fault logging system is used for information security event reporting procedure
c) Central fault logging system ensures all employees of information systems and services note and report any observed or suspected security weakness in the system or services
d) Monitoring of systems, alerts and vulnerabilities are used to detect information security incidents.

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

3.9.2 Incident response procedures

a) Management responsibilities ensures quick effective and orderly response to information security incidents
b) Information security incidents are addressed by respective persons of ITC.
c) Priorities are set on the basis of criticality and business requirement.

3.9.3 Learning from information security incidents

a) Analysis is being done to identify cause and quantify the type, volume and costs of information security incidents.
b) Analysis of the past information security incidents are used to prevent recurring or high impact incidents.***3.10 Business continuity management***

3.10.1 Developing and implementing continuity plans including information security

a) Online backup at remote site is used to maintain and restore business operations, ensure availability of information within the required level in the required time frame following an interruption or failure to business processes
b) Business continuity procedure considers identification and agreement of responsibilities, identification of acceptable loss, implementation of recovery and restoration procedure, documentation of procedure and regular testing.
c) All major online data is transferred to remote location under Disaster Recovery Project (DRP) by OFB Kolkata.

3.10.2 Testing, maintenance re-assessing business continuity plans

a) Business continuity plans are tested regularly to ensure that they are up to date and effective.
b) Business continuity plan tests ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security by viewing various log files on server.

3.11 Compliance

3.11.1 Legal compliance

Servers are centrally purchased by OFB, Kolkata, along with the licensed

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**

software. Desktops OS license is bought along with the hardware. Inventory of software is maintained according to name of software, license number and type of software.

3.11.2 Policy compliance

ITC is covered under ISO 9000 audit and all the documents are subject to audit. The documents are reviewable for the improvement of any process on requirement basis.

3.11.3 Technical compliance

Each and every equipment/electronic gadget is checked periodically during preventive maintenance as per schedule of each HW/SW/Applications.

Approved By:	Checked By:	Prepared By:
N.K.Sinha	**R. K. Tiwari, Jt GM (CP)**	**Satya Sawroop**
General Manger	**Information Security Officer**	**HOS/ITC**