eGov@Gujarat

- An *e-Governance* Bulletin from GUJARAT INFORMATICS LTD.

Vol. 10 | No.1
June, 2013

Information Security

Information Security

- **Introduction**
- **Background**
- **What is Information Security?**
- **What is CIA?**
- **Is Information Security only IT Security?**
- **Desktop & Laptop Security**
- **Virus Protection Password**
- **Security Internet & Email**
- **Security Data Protection**
- **Information & Media Handling**
- **Social Engineering & Incident Reporting**
- **Physical Security**
- **Security Violations**
- **Enforcement**
- **eGovernance News**

Courtesy By

Shri S.J. Haider, Secretary, Science & Technology Department, Govt. of Gujarat

Editorial Team

Dr. Neeta Shah
Mr.Amit Barot
Mr. Sanket Prajapati

Information security analysts are information technology (IT) specialists who are accountable for safeguarding all data and communications that are stored and shared in network systems. In the financial industry, for example, information security analysts might continually upgrade firewalls that prohibit superfluous access to sensitive business data and might perform defenselessness' tests to assess the effectiveness of security measures. Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)

Two major aspects of information security are:

IT security Sometimes referred to as computer security, Information Technology Security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory (even a calculator). IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance The act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to; natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arises.

Background:

A security strategy has been outlined by DeITY (GoI) to address the strategic objectives for securing country's cyber space and is being implemented through the following major initiatives:

Security Policy, Compliance and Assurance Security Incident Early Warning & Response Security training skills/competence development & user end awareness. Security R&D for Securing the Infrastructure, meeting the domain specific needs and enabling technologies Security Promotion & Publicity.

What is Information Security?

- Securing information
  - One who doesn't need to know it shouldn't know it
  - One who doesn't need to change it shouldn't be able to
  - It's there for me to know or change when I want to!!

In other words…

> The protection of information and information processes systems against unauthorized access to or modification of information, whether in storage, processing or transit.

What is CIA?

- The 3 Pillars of Information Security
  - **Confidentiality** : ensuring that information is accessible only to those authorized to have access
  - **Integrity** : safeguarding the accuracy and completeness of information and processing methods
  - **Availability** : ensuring that authorized users have access to information and associated assets when required

General Use and Ownership

- User should remember:
  - Data you create on the corporate systems remains the property of Gujarat State Data Centre (GSDC)
  - Users are responsible for exercising good judgment regarding the reasonableness of personal use
  - GSDC reserves the right to audit networks and systems on a periodic basis to ensure compliance with the program
  - Authorized individuals may monitor equipment, systems and network traffic at any time for security and maintenance purpose

Desktop & Laptop Security

- Feeling tired, bored – want to take a break:

  CTRL+ALT+DEL
  - Try this: Enable Screensaver Password with time parameter of 1 min

- I want to install Google Earth or computer Games??
  - Use only GSDC preapproved software

Always remember that any other software installation requires approval from concerned Authority

- Want to change the hardware settings
  - Do not do it, you are not authorized to do it

- Do maintain the proofs for approved changes in hardware / Software

- Want to connect own laptops / mobile phones to GSDC network
  - Do not do it, take permission from CISO (Chief Information Security Officer) if absolutely necessary
  - Do not use external devices unless it is approved by concerned authority

- Do not use the license keys owned by the GSDC for personal use or Circulation within or outside the GSDC
  - It can lead to legal liabilities

- Make sure that the third party personnel should not access the GSDC's systems unless authorized for business purpose.

- To prevent the risk of unauthorized access, users should:
  - Laptop users should use power-on passwords
  - Users with authorized access to LAN should not connect to Internet through personal modem / Wi-Fi simultaneously.
  - Users should ensure that login process is followed using their account ids and strong password.

- All sensitive information on laptop should be secured either through password protection or by using encryption.

- Users using external internet connections on laptops shall ensure that
  - Anti-virus signatures are updated
  - Personal firewalls are enabled on laptops
  - Latest security patches are installed

- Have you ever lost your files/data/folders:
  - Do take backup at regular intervals
  - Take backup of important files in the secondary partition i.e. D: /

- Theft of systems
  - concerned personnel shall file a police report and subsequently inform the administration department

- Feel like stopping the antivirus scan:
  - No, don't do it.
  - All the external resource data should be scanned for virus before opening

Virus Protection

- Ensure that antivirus on his/ her workstation is updated
- Promptly communicate to their immediate supervisor/ senior, if they discover any security incident (like virus infection, unusual activity, passwords shared etc.)
- Never open attachments from unknown sources
- Do not use any external source such as CDs; USB drives etc. on GSDC technology infrastructure unless scanned for viruses, and approved by the department head

Password Security

- Use your unique ID for accessing GSDC information assets
- Adhere to the password policies of GSDC as listed below:-
  - Passwords should have a minimum length of eight (8) characters
  - Password should have alpha numeric characters
  - Passwords should be changed once in 45 days
  - A maximum of five successive login failures shall result in a user's account being locked out
- Do not use shared accounts for accessing GSDC's information assets
- Never share their passwords with anyone
- Never write down or paste passwords in public spaces or at the workplace

Internet Security

- Internet is for official purpose only,
  - Research, work and learning
  - Administration
  - Official activities.
- Connect to Internet through LAN & not using MODEM or personal Wi-Fi
- Do not download software's which are not approved by GSDC
- Ensure that all downloads (documents, email attachments) are scanned for virus before opening.
- Do not blindly click on pop-ups, do not click on the links while giving financial information-- type the URL
- Remember: You are responsible for protecting your Internet account and will be held responInternet is for official purpose only,
  - Research, work and learning
  - Administration
  - Official activities.
- Connect to Internet through LAN & not using MODEM or personal Wi-Fi
- Do not download software's which are not approved by GSDC
- Ensure that all downloads (documents, email attachments) are scanned for virus before opening.
- Do not blindly click on pop-ups, do not click on the links while giving financial information-- type the URL

sible for any misuse of Internet access originating from your account

- Users should not use Internet facilities -
  - To play games or access games
  - To access offensive materials
  - For personal financial gains
  - To print or save any copyright protected material
  - To download entertainment materials
  - To hack / attempt to hack other systems- internal or external
  - Creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin
  - Download or distribute malicious software or tools or to deliberately propagate any virus.
  - Download non-business related content like images, music and video files.
  - Violate any copyright or license agreement by downloading or distributing protected material
  - Upload files, software or information belonging to the GSDC to any Internet site without authorization of the owner of the file/ software/ information
  - Share any sensitive information of the GSDC with any Internet site unless authorized
  - Post views or opinion on behalf of the GSDC unless authorized
  - Post remarks that are defamatory, obscene or not in line with the GDSC's posture on the subject. Conduct illegal or unethical activities
  - Do not send/ receive/ view racial, sexually threatening, defamatory or harassing messages
  - Do not use any kind of Internet chat services like MSN messenger, Yahoo chat, Rediff chat and social networking sites like Orkut, Face book etc

- GSDC has the right to monitor the Internet usage of the users. In case such misuse of the Internet access is detected:
- GSDC can terminate the user Internet account and take other action as deemed fit by the management/ decision making authorities on the subject

Email Security

- Use your email id only for official purpose
- Email Can be Legally Binding
- Do not express personal opinion in official mails
- Do not mention your official email address in mailing lists
- Do not post/share CONFIDENTIAL/RESTRICTED information over e-mail while communicating with external entities unless explicitly authorized by concerned authority
- Encrypt and password protect the sensitive information contained in attachments
- Secure your mail account with strong password and do not share that password with any one

- Your email is as official as your office letter head.
- Do not reply to SPAM mails, instead report it to the helpdesk
- Do not send chain mail and SPAM mails
- Attachment with the mails:
  - Attachment with the following extension should be considered malicious:
    - .jpg.vbs, .txt.shs, .pif, .exe, .shs, .vbs, .chm, .com, .scr, .hta, .hto, .dll and .bat.
    - Take necessary precautions while opening email from unknown person

Archive mails and take regular backups

- The GSDC reserves the right to monitor e-mail messages and may intercept or disclose or assist in intercepting or disclosing e-mail communications to ensure that e-mail usage is as per this policy.
- Users must not automatically forward their e-mails to any address outside the group / company networks.
- Blanket forwarding of e-mails and transmission of chain messages is prohibited.
- Do not use e-mails within the organization to harass Users
- Do not communicate with any third party which may potentially invite involvement of law enforcement agencies
- Do not participate in chain e-mails
- Do not forward sensitive e-mails containing GSDC information to the external world, even inadvertently
- Do not register GSDC e-mail addresses on external websites

Data Protection

- Users shall understand business/ contractual requirements of data protection from their respective managers or departmental heads.
- Classify information assets according to their level of sensitivity and handle the same accordingly
- Protect vital physical records which contain business related information
- Take periodic backup of data (mails, personal folders etc.) on a regular basis
- Do not send business data related to the department to any third party

- Do not use camera mobile phones in secured areas like server rooms
- Users shall not leave confidential documents on the desk; instead it should be kept in a locked cabinet
- Do not leave printouts unattended at the printer machine
- Do not reveal information about GSDC's business details in white papers or presentations
- Never discuss official matters in public places

Information & Media Handling

- Label all the removable media like USB, CD, floppy or DAT tapes
- Printouts are collected immediately on firing the print job.
- Documents are not faxed to unattended / unknown fax numbers/ e-mail boxes.
- Do not share your laptop/USB devices with other persons
- Securely store the CD-ROM, Floppy Disks and other storage devices
- Shred the Paper documents while disposing
- Destroy the CD-ROM/Floppy Disks while disposing
- Use external media for business purpose only

Social Engineering

- Do not discuss sensitive information with others
- Do not give out sensitive information over email/telephone
- Do not leave sensitive documents on your desk/printer/fax/ public places

Incident Reporting

- It is the responsibility of each employee to report any observed or suspected information security incidents and/or weaknesses to the helpdesk telephonically and by email to support@gujarat.gov.in
- Users shall be informed that they should not, in any circumstances, attempt to prove a suspected weakness. Any action in testing the weakness shall be interpreted as a potential misuse of the system.
- Users shall not discuss with colleagues about the suspected weakness once it is reported to higher authority for investigation.
  - Report
    - E-mail id: support@gujarat.gov.in
    - Phone : 079 – 23251096
  - Examples of the incidents:
    - Suspicious system activity
    - Virus infection
    - Degrading system performance
    - Unauthorized deletion of data
    - Escalation of privileges
    - Violation of policy by others

Physical Security

- – ID Badges shall be displayed all times within GSDC premises
- - Users shall participate in safety drills organised by GSDC
- - ID Badge should be carried in such a manner that it is visible at all times
- - Do not tailgate or allow tailgating in secured areas like server room
- - Do not lend or borrow access cards
- - Do not disregard safety instructions
- - Escort your visitors
- - Lock all the important documents

Security Violations

- A security violation is any attempt to breach the security of applications, network and IT devices, whether or not it results in actual damage or financial loss.
- All security violations will entail disciplinary action

  o The following are examples of security violations

- All security violations will entail disciplinary action trade secret, patent or other intellectual property, or similar laws or regulations
- Unauthorized copying of copyrighted material
- Using a GSDC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication.
- Unauthorized hardware or software changes

Enforcement

- Any employee found to have violated this implementation toolset may be subject to disciplinary action, up to and including termination of employment.
- Contact Information:
- For information regarding this toolset, contact GSDC.

e Governance News

eMaharastra Awards 2013

- e-Maharashtra Awards has been instituted with the primary aim of felicitating and acknowledging regional initiatives in the use of ICT in Government and Education. The e-Maharashtra awards will be instrumental in promoting the most innovative initiatives in the domain of ICTs for Development and to spread awareness about the role of ICTs in addressing social concerns. The Awards ceremony will felicitate efforts made in Maharashtra though the innovative use of ICTs.

- Our aim is to identify and popularise emerging leaders and innovative projects from different sectors of the development community, including the grassroots organisations. The Awards are open for all national and international organisations, civil society organisations, bi-lateral, multi-lateral developmental organisations and enterprises working in Maharashtra who have transformed social development opportunities into a sustainable social enterprise through innovative use of ICTs. The Award winners will be felicitated at the e-Maharashtra Leadership Summit 2013.

- The e-Maharastra Awards 2013 ceremony was held on May 09-10, 2013 at Taj Vivanta, President, Mumbai. Gujarat has won the following major awards:

Sr. No.	Winner	Category
1	Information Technology Center, University Bhavan , AAU	e-Krishi Kiran Programme (Soil Health Card)
2	National Informatics Centre, Gandhinagar	XLN – Xtended Licensing & Laboratory Node (Best Government to Business (G2B) Initiative of the Year)