Sri Lanka Sentry

Guidelines on Information Security

ICT Agency of Sri Lanka

eSri Lanka
smart people smart island

ICTA
ideas actioned

Sri Lanka Sentry:

Guidelines on Information Security.

Information and Communication Technology Agency of Sri Lanka (ICTA)
# 160/24, Kirimandala Mawatha,
Colombo 05,
Sri Lanka.
Telephone : +94-11-2369099
Fax : +94-11-2369091
E-mail : info@icta.lk
Web : http://www.icta.lk

Introduction

The Government of Sri Lanka launched the e-Sri Lanka program, in November 2002, with the objective of using ICT in all its aspects for the benefit of the people of Sri Lanka and to further the socio economic development of the nation. The e-Sri Lanka roadmap resulted in the implementation of the Information and Communication Technology Act, No. 27 of 2003, under which the Information and Communication Technology Agency of Sri Lanka, (ICTA), is operational. ICTA is the implementing organization for the e-Sri Lanka initiative.

The overall objective of the e-Sri Lanka program is to take the dividends of ICT to every village, every business and every citizen in Sri Lanka. This is to be achieved through the following strategies:

- o *Developing ICT Human Resources.*
- o *Building the National Information Infrastructure:*
- o *ICT Investment and Private Sector Development:*
- o *Creating an empowered knowledge based society (e-Society).*
- o *Re-engineering Government: delivering citizen Services:*

The implementation of the Re-engineering Government program would result in Government agencies being able to work together more easily, electronically, and information being reusable from one agency to another. Government agencies will be connected through the LakGovNet Project and information will be electronically shared across agencies; and also databases with personal information pertaining to citizens, will be established. Therefore Government agencies will need to balance between giving employees real-time access to applications and information, and addressing the corresponding concern for the security of information and the information systems. Balancing these needs necessitates secure information systems.

Thus, information security should not be regarded as only a technical issue but as an integral part of all organizational activities and business process. The need for information security should be prioritized in all present and future activities of your organization. As a first step in implementing security, employees should be provided with awareness, and given regular updates on security policies and best practices.

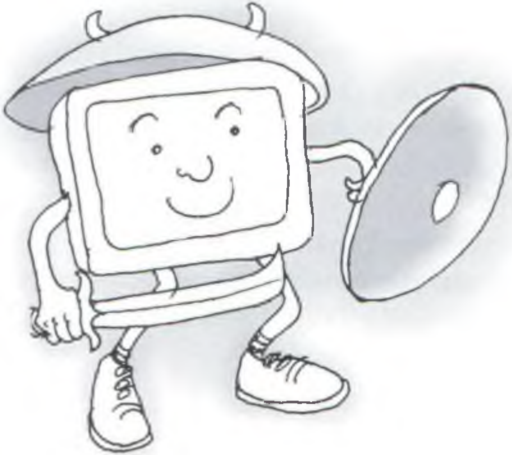
With this objective in mind ICTA's *Information Security Working Group* has drafted *Sri Lanka Sentry: Guidelines on Information Security*. This is meant as a basic user guide which gives the necessary awareness and knowledge for an end user to ensure security in his/her organizational activities. These Guidelines are meant to be Best Practice and should be implemented whenever possible so as to assure basic uninterrupted security for your information systems

Information Security Working Group,
Information and Communication Technology Agency of Sri Lanka (ICTA)
November 5, 2004

Sri Lanka Sentry :
Guidelines on Information Security

Scope:

This guideline / best practice is meant for end users of information and communication technology (ICT) systems. It should be used in accordance with the policies, guidelines and regulations of the organization where you are employed.



Need of a guideline / best practices:

One of the organizations most critical assets is its data and information. Therefore protecting an organization's data and information from access by those not permitted to do so (unauthorized access), use, change and destruction is of vital importance. ICT security refers to the protection of assets from unauthorized access, use, alteration and destruction. It includes protecting against unauthorized data disclosure and ensuring the authencity of the data source, preventing unauthorized data modifications and preventing data delays or removals. All ICT systems can be affected by security breaches but security breaches can often be easily prevented. An insecure system is a threat to other systems and insecure machines can fall under the control of an outside hacker.

The result of a security violation can range from mere annoyance to complete incapacity: Important data can be lost, intellectual property rights (IPR) can be breached, privacy can be violated, and a computer can even be used by an outside attacker to attack other computers on a network. Threats to the secrecy and integrity of data and denials of access and data removals are usually carried out by a small minority. But the damage done by a single hacker can have huge consequences on ICT systems. Therefore knowledge of how to protect an organization's ICT systems is essential.

This guideline provides you with best practices and steps you can take to protect computers against security threats and ensure that systems are safe and cannot easily be used to attack other computers on a network.

Intrusion prevention

> *Sunethra, as the CEO of the ABC Corporation had to take the decision – Nalin, the web developer had to be dismissed. He had made too many mistakes too many times She would appoint Suren, who had been working as Nalin's assistant for about 6 months, as the new web developer. Suren seemed capable of running ABC's website and implementing the necessary security. Two weeks later ABC announced the launch of a new product. For further details, Sunethra informed the press "contact the website". The following morning a cyber vandal had defaced the site, replacing the site's regular content and information about the new product, with gruesome and offensive graffiti.*

An intrusion occurs when someone breaks into and gains access to a system. Intrusion can be physical or electronic. Intruders can be from outside an organizations network, or could be employees of the organization who can legitimately use the organization's equipment and network, and misuse the privileges given to them.

(a) Physical access

- **Positioning your monitor:**

Position your monitor in such a way that people walking into your organization cannot – either intentionally or unintentionally – view what is on your screen. Information thus gathered accidentally by those outside the organization can sometimes lead to negative repercussions.

- **Assets under your purview:**

Clarify from your senior officer what information, software and assets you are accountable for, and immediately report any malfunctions to your senior officer or to the person designated, to whom such incidents should be reported.

- **Safeguard your equipment:**

  - Don't leave devices on which you save information storage devices such as disks and memory sticks unattended where these can be taken away by unauthorized persons. Visitors to your organizations, if ill intentioned, could easily walk away with such a device and get access to information saved on the device.

  - Store laptops, PDAs, and other hardware devices in a secure,locked place when not in use.

  - As far as possible avoid taking equipment in which sensitive information is stored, away from the office, and also try not to use your laptop etc., and work with sensitive data in public places.

  - If your organization allocates another computer to you, and sends the one you have been using to another section or away from the office, ensure that the information stored in the computer you were using, unless needed by another section of your organization, is erased.

- **Lost, damaged or stolen items:**

  If any items such as disks, memory sticks allocated for your use are lost, stolen or damaged you should immediately report it to the help-desk or to the designated responsible officers.

- **Authorization:**

  If you take any ICT equipment other than a lap top or mobile phone assigned to you by your organization, then you should obtain authorization for removal from the officer responsible for custodian functions of such equipment.

(b) Electronic access:

- **Use passwords:**

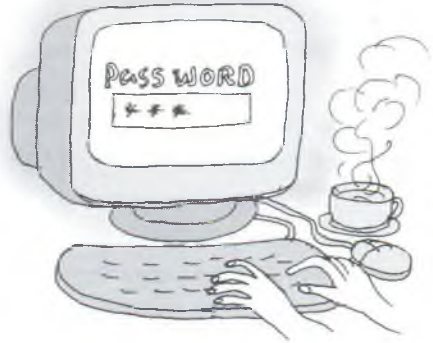
First make sure that your ICT systems are password protected so that only those who are authorized can enter the system or parts of the system.

Never use your login name in any form – e.g. reversed, in upper case - as its password.

Do not use easily guessed passwords, such as your name, your name backwards, your spouses' names and children's names or the name of your organization.

Ensure that initially assigned passwords for any system you are using are changed upon first login.

Do not use words found in dictionaries as passwords, as software exists specifically designed to crack passwords. "Dictionary attacks" involve trying out all the words contained in a dictionary. Ready-made dictionaries of millions of commonly used passwords can be freely downloaded from the Internet.



Do not use key-board patterns such as "*qwerty*", as your password.

Change passwords regularly, at least once in three months.

Keep passwords secret - never divulge your passwords to anyone.

If you do need to write down your password keep it in a secure place, preferably offsite.

Do not keep passwords in shared drives.

Make passwords as meaningless as possible, and mix letters and numerals in the password.

Don't use the same password in more than one place.

Let your password have a minimum of 8 characters as an intruder may try all possible combinations of characters to break a password, and a longer password will take longer to crack.

Do not use passwords of former employees who may have held your post before you.

If your password is re-set by a network administrator, ensure that you change it or ensure that you are the only person who knows what the password is, from that point onwards.

If you use remote access to your organization's servers, be especially sure not to share dial up passwords given to you with other employees or with outsiders.

- **Choosing a good password**:

Use a mix of both alphabetic characters and numerals.

In your alphabetic characters, use a mix of uppercase and lower case letters.

Choose, for instance, a middle line from a little known song or poem and intersperse with numerals.

Choose a phrase or a combination of words that you will remember – one that has some meaning for you – so that you won't have to write it down.

Choose a password that you can type quickly so that, someone watching over your shoulder will not be able to glean what it is.

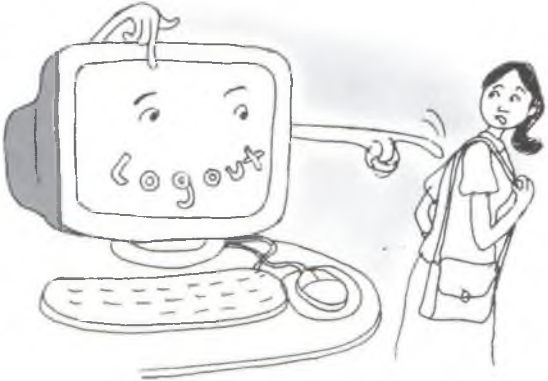
- **Screen savers:**

  Ensure that you use a password protected screen saver, and set the wait time as less than 10 minutes.

- **Log out:**

  Do not leave your PC logged on. You should log out and switch off your PC, before leaving at the end of the day, unless an overnight process is being run on it. (even if you are not at your desk)

Virus and malicious code:



The National Apex body on ICT made another announcement on television about the Chernobyl virus. The following morning, at the Department of XYZ an announcement was made over the public address system "Don't switch on your computers". Sunil the Accountant had been working at the Department for over 30 years – mostly on manual systems. He refused to believe that a virus could really do harm, in spite of the awareness programs conducted by the Department. Of course he switched on his computer, in spite of the warnings from his staff, and lost all information he had in it. He was keying in the information for at least three months thereafter.

Hundreds of thousands of computers in Asia and the Middle East had their data wiped by the malicious Chernobyl virus on 26 April 1999 - the anniversary of the Ukrainian nuclear disaster in 1986. The virus deleted most of the data stored on computers and can even wipe out the BIOS - the basic instructions that tell the computer to start. Chernobyl was less widespread than the e-mail replicator virus Melissa, but it with more serious impact, especially on Windows 95 or 98 machines. Police in Taiwan questioned a computer expert, graduated from Taipei's Tatung Institute of Technology, who they say has admitted creating the Chernobyl virus, which caused this major disruption. In Taiwan, intentionally spreading a computer virus is an offence.

Viruses are computer programs written with malicious intent designed to replicate themselves and infect computers when triggered by a specific event. Virus infections occur through email attachments, from files downloaded from the Internet and from disks. The consequences of virus attacks can range from being merely causing annoyance to being more destructive such as slowing down systems and deleting data.

Use up to date virus protection software:

Ensure that virus protection software is installed in your server/ computer and it is essential to update the software regularly. Check your anti-virus software website for sample descriptions of viruses and to get regular updates for your software.

Don't open emails / attachments from unknown sources.

Do not open any attachments on emails from unknown sources or attachments on unsolicited emails. Worms are sent through personal address books and this precaution is recommended even if you know the origin of the email. If a suspicious email is received it would be best to delete the entire message, including attachments. Even if the origin is known care should be taken if the message looks strange and unexpected.

Regularly download protection update patches.

Ill intentioned persons could attack your systems through bugs in a program and software companies create patches which they post on their web sites to defend against bugs. Check your software web site regularly for new security patches and be sure to download and install the patches. You could also download and install a utility program to do this for you.

Turn off Preview.

Whatever the email software you use, turn off the preview function.

Show Extensions.

Set all programs to show you the full file name, particularly E-mail programs.

If your program drops the extension you don't know if the attachment is executable or not, and this can be used by ill-intentioned persons to disguise virus programs as some other file formats, such as text, video or audio files. For example, the VBS/LoveLetter worm contained an e-mail attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs". If you had extensions turned off you would have seen the attachment as "LOVE-LETTER-FOR-YOU.TXT" which you would have thought, was a harmless text file.

Protect Floppies. (and any other movable devices)

Write-protect any floppy disk you place into another person's computer.

Be careful of hoaxes:

These are false messages claiming to be a new virus circulating.

Do not delete anti-virus software:

You should not under any circumstances attempt to disable or delete virus protection software on your computer.

Do not install unlicensed software

Do not attempt to install unlicensed software on to your computer from the Internet or from any other source.

- **Turn off file sharing:**

  The ability to share the files on your computer can be used for unauthorized access by ill-intentioned persons. Data can be accessed, modified or deleted and viruses can be introduced. Therefore unless you really need to use this ability, turn off file-sharing.

- **Monitor Active content:**

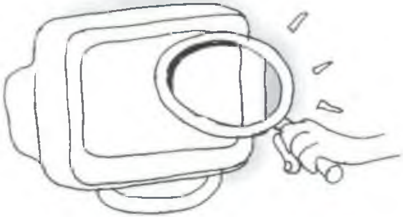
  Active content is downloaded when you use your web browser and view a web page containing active content. These are programs embedded in web pages which provide animation and dynamic content to web pages and in most instances are harmless.

  However, ill-intentioned persons can embed malicious active content in seemingly harmless web pages which could then send back information from your PC, or cause destruction of varying degrees to the information on your computer. Both popular browsers- Microsoft Internet Explorer (IE) and Netscape Navigator - can recognize when they are about to download active content.

  Set your browser so that you can control whether active content is to be downloaded to your computer or not. Also set your browser to verify the identity of downloaded active content.

- **Monitor cookies:**

  Cookies are small pieces of unencrypted text stored in client computers by web sites that you visit and used by marketing firms to gather and track user's visits to web

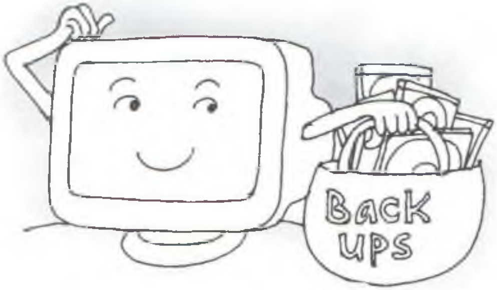


sites. Cookies may contain information such as passwords, login information and details of web sites you have previously visited; cookies do not directly harm client machines.

Set your browser so that it asks whether to store the cookie without warning, receive a warning that a cookie is about to be stored, or you could set it to disallow cookies altogether.

Backups and recovery

Surani was at her computer in 1996 when a bomb destroyed sections of the Central Bank of Sri Lanka, Colombo. She ran out and saved her life, and later realized that only some printouts of the EPF records that were currently being processed were left at the Central Bank, Colombo, premises. In addition to the devastating loss of lives, more than 7 million EPF records kept electronically were destroyed. Once normalcy was restored this would have been a crucial problem. But backup tapes of the critical EPF information were kept at the Central Bank branch at Rajagiriya and what would have been a major crisis for the country was thus averted.



Back ups of the important information needed for the organization should be taken regularly, so that the information is available in the backup in case the original is lost due to a disaster, or a power failure etc. A minimum level of backup information should be kept in an off-site location in case the information at the main site is destroyed or damaged.

- **Take regular back ups:**

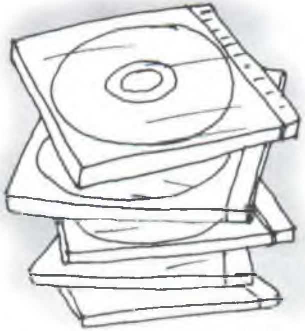
  Ensure that you take systematic and regular backups.

  Ensure that your backups can be read on systems other than the one in which you created them.

  Ensure you have your original software start-up disks available in case your computer system files get damaged.

  Back up on floppy disks, CDs or USB flash memory storage-depending on the amount of data of which you are taking a backup - or on another computer in the network.

  Write protect disks when storing.



Store backups in a different location from the original computer system. Consider storing backups of crucial and important information and web sites at an off-site location. Ensure that all critical data/information is backed up, if your computer is sent away from the organization for repairs.

Label your backups on content and date.

Implement a backup plan for your organizations servers/PCs.

- **Security of your equipment:**

  Ensure that you have a UPS (uninterruptible power supply) system.

  All sensitive/confidential data residing in desktops/laptops should be removed before sending such machines for repairs. Where possible the respective hard disks should be removed.

Best practices

- Email

Your organization may be using emails for business communications, replacing traditional forms of communications such as paper letters. You should be careful of minimizing security risks through using emails.

Ensure that you address your emails correctly, i.e. ensure that the recipient address is correct. If not, you may send organizational information to those who should not be receiving such information.

Do not send or forward defamatory, offensive or obscene messages using your organizational email, nor should you use it for harassment – you should be careful of not compromising your organization.

Do not use your office email for unauthorized purchases.

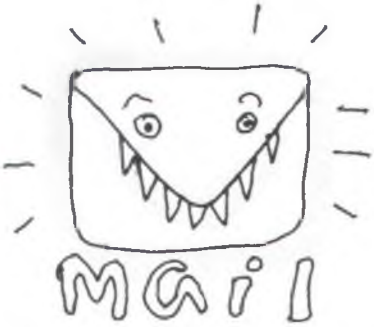
Check with the recipient before sending very large attachments.

Do not send exe files.

It is best to send personal and confidential information through a personal email address rather than use your organizational email address for such purposes.

Do not forward chain letters.

You should keep messages to the point and relevant and read through the message carefully, before you click on "*send*".



- **Be wary of scams**

Scam emails may request personal information, credit card information etc. pretending to be, for example, a billing request; or an email contain links to website which may request such personal information. Malicious web sites too are used to collect visitor's information; credit card numbers etc., or download viruses.

Do not give out personal information, passwords, credit card information etc., online. Refrain from registering for contests, lotteries through false web sites.

- **Guard against spam:**

Spam refers to unsolicited emails and unsolicited advertising through emails. Spam does not directly harm your systems but may be an annoyance and may take up storage space on your computer. Check whether the mail directs replies to an email in another domain.

Don't post your email address on web sites.

Don't reply to spam, simply delete the messages.

In the case of web based emails, such as Yahoo, there are built-in anti spam reporting and preventing mechanisms, which you can use.

Don't click on links and open web pages on spam emails as this would confirm your email address.

When completing and sending out web forms you may need to uncheck check boxes which may be checked by default. If you do not uncheck the boxes you may inadvertently be requesting information without realizing it.

Do not use 'removal' links included in emails.

Prevent cyber-stalkers:

Shanika met the perpetrator in a chat room and made the mistake of giving him her office email address and other contact details. When she realized her mistake it was too late. He started sending emails with propositions but she continually rejected his attempts, and blocked his email from the server, but he kept opening new (web based) email addresses. The perpetrator, a forty-two-year-old unemployed person retaliated to her rejection by posting her personal details on the Internet. These included her physical description and *telephone number. She got dozens of calls from various people and developed a fear of going outside of her house.*

Cyber-stalking, is an extension of physical stalking, where electronic media such as emails and the Internet are used to contact, pursue, harass or proposition another in an unsolicited manner.

If you are being stalked online ensure that it is not taken off-line - do not give your physical address, telephone number to people you talk to.

Do not respond to the stalker.

In the case of email harassment report the stalker to the stalker's ISP (Internet Service Provider).

If the problem only exists on ICQ, MSN or other such program, then go offline immediately.

Consider changing your online identity.

Stay out of chat rooms where problems could be triggered.

Ensure not to give out personal information through which you could be identified online.

- **Be apprised of your security policies:**

Organizations both large and small concerned about protecting their ICT assets should have a security policy in place.

A security policy should address physical security, network security, access authorization, virus protection and disaster recovery etc. In addition to being a set of written regulations by which an organization operates, a security policy could comprise rules that are electronically programmed and stored within computer security equipment. You should contact your superior officers and be apprised of the contents of your organization's security policy.

- **Be aware of your organization's disaster recovery plan:**

Your organization's disaster recovery plan should include the assessment, prevention and minimizing of risks, and minimizing interruptions to work, backup plan and cost effective solutions, recovery of lost data.

You should contact your superior officer be also aware of your organizations' disaster recovery plan, so that you will know what you should do in case there is a security breach, virus threat etc..

- **Your organization's regular security inspection**

  When your organization assesses potential risks for future events, try to be aware of the outcome – contact your superior officer about this. Your organization should evaluate the security of its ICT systems comprehensively and regularly - at least twice a year, and implement cost-effective strategies.

- **Participate in training:**

  As an employee you should know what to do if your computer becomes infected, so that a virus does not spread to other computers on your LAN and to outside networks, and training should be provided for employees to update them with disaster recovery scenarios. Find out from your senior officers when such training / awareness programs are held and participate in these programs.

An organization should have a security forum which gives direction and support for the security initiatives in the organization. It would be the responsibility of the forum to provide the necessary human and other resources for the implementation of security and the forum should be part of an existing management body. The forum would review and approve the security policy of the organization, review threats and security incidents and there should be one person responsible for the overall security.

Reference:

1. E-Commerce – Gary P. Scheider & James T. Perry
2. ISO / IEC 17799 – Information technology – code of practice of information security management.
3. www.staysafeonline.info – sponsored by the National Cyber Security Alliance, USA.
4. Security basic best practice for users, Denis A Nicole, 2003-12-22
5. Best Practices and Assessment Tools to promote cyber security awareness. http://www.cscic.state.ny.us
6. Crime library; criminal minds and methods - www.crimelibrary.com
7. www.antichip.org

Information Security Working Group.
ICT Agency of Sri Lanka (ICTA)
November, 2004