Nreach encourages all users and administrators to adhere to the following basic security " best p ractices" :

Threats to computer systems worldwide are continuing to increase. Whilst Staff in AACS and local IT Support Staff makes every effort to provide a secure environment for our computers, it is true to say that the network is only a secure as it's weakest link. This means that we require the cooperation of every user in our community, and every person who manages their own workstation to help us out by adopting the best practice working methods that we recommend.

- On this site we you will find a guide to best practices and details of the Antivirus software available for use by Staff and Students.
- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Do not open any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
- Try not to use "CC" to send emails to multiple recipients. It increases the possibility of spamming. You can send mails to peoples by using "BCC". Make it a practice and tell others to get used to.
- Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- Do not download any files from strangers.
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.
- Update your anti-virus software regularly. Over 500 viruses are discovered each month, so you'll want to be protected. These updates should be at the least the products virus signature files.
- You may also need to update the product's scanning engine as well.
- Back up your files on a regular basis. If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.
- When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats. Check with your product vendors for updates that include those for your operating system web browser, and email.
- One example is the security site section of Information Services Network Limited located at **http://www.nreach.net/virusalert.html**

- Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, telnet, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.

- If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.

- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.

- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.

- Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.

- Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.

- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.