APPENDIX B - INFRASTRUCTURE SECURITY FOR SCHOOLS GUIDELINES

It is essential that all users of the network are aware of the strategies used to protect the security of the data to which they have access.

B.1. SECURITY SETTINGS

The security settings are designed to:

- establish trust levels;
- limit the ability of people to guess passwords;
- assist in the maintenance of a secure network structure;
- assist with detection of security breaches; and
- maintain effective security.

Any person with administrative privileges can change the settings. Regular checks are essential to confirm that unauthorised changes have not occurred such as changes made without authority or through an attack over the internet via phishing, viruses or spyware.

Details of the correct settings can be obtained from the Customer Service Centre. It is highly recommended that these settings be followed to increase the security of any school managed networks. Print out the details of settings on your network and keep them in a locked secured container.

Secure network devices, both physically and logically, as many security breaches are preceded by unsuccessful attempts. If those attempts are detected and acted upon early, the chances of their success can be greatly reduced.

Network access logs need to be checked regularly. The principal, in consultation with the school's network administrator, should evaluate the risks at the particular site before deciding the frequency of checking. Note that the logs are to be retained in accordance with the *State Records Act*, as detailed in the *Records Management Manual for School, College and Campus Records.*

The following frequencies are recommended:

- **All sites:** network access logs should be checked at least monthly to maintain an understanding of the normal level of errors, to check that logging has not been turned off and to maintain skill levels.
- **Sites with a moderate security risk:** sites previously identified as a moderate security risk should check their network access logs weekly.

Curriculum Network administrators should note the frequency of errors and investigate any instances they consider to be suspicious.

Action
ICT Coordinator or person nominated by the principal to arrange for the logs to be checked monthly or weekly depending on assessed risk level.

B.2. EXIT PROCEDURES

The establishment and correct application of proper exit procedures:

- confirms staff who cease employment no longer have an active account;
- prevents the disclosure of logon and password by staff no longer employed by the Department; and
- prevents the misuse of an account once a staff member has ceased employment with the Department.

Network administrators are immediately advised when a person ceases working at a school and confirm that access privileges are disabled.

Action

- *The principal should confirm adequate exit procedures are in place.*
- *Twice a year, the principal should have the network administrator create a list for review of all logons with the date last used.*
- *The school network administrator/ICT coordinator to distribute the list to the principal and deputies, asking them to provide the names of people who have left the school. Keep a copy on file.*

B.3. SECURITY GROUPS

The risks of a security breach are greatly reduced by granting network access on "need-to-know" principles. If every person at a work site has access to sensitive data, it takes only one careless person to leave the school network at risk of unauthorised penetration.

The network security system provides for logons to be placed in security groups. Security privileges are then granted to the groups as needed so that access to some information is restricted to members of a group, rather than being available to the entire school.

People can be members of more than one group. It is advisable to arrange security groups on the curriculum network as follows:

- Teaching staff – various levels but could include principal, deputies, teachers, school psychologist, 3rd party support contractors, etc.
- Various levels of students

School ICT Coordinators should arrange membership of security groups to reflect the needs of the school. This is done by first defining the type of standard access that will be given to people with different roles. The role of an individual is carefully defined when he or she receives a logon.

Reviews should be carried out annually by giving the principal or other reviewing officer details of what curriculum network access has been granted.

B.4. LOCATION OF SENSITIVE INFORMATION

Because of the risks of intrusion and wrongful disclosure, it is advisable to occasionally check the type of sensitive information held on servers and workstations.

Principals should nominate staff to carry out these reviews.

It would be worthwhile for the reviewers and the custodians of sensitive information to be aware of the requirements and principles outlined in the *Records Management Manual for School and Campus Records.*

Action

The principal should conduct an annual review of the location of sensitive information by:

- *appointing one or two people to request staff to describe the type of confidential information they have stored on the network; and*
- *have the reviewers advise on alternative methods of storing and protecting that confidential information e.g. encrypted folders, password protected folders, limited access folders.*

B.5. NETWORK OPERATING SYSTEM

There are many well-known and easily available techniques which can be downloaded from the internet for breaking into networks that use old software. There are also many malicious individuals working together to exploit security vulnerabilities as soon as they are discovered.

Exploitation of vulnerabilities. Security vulnerabilities have in the past been found in operating system, email, browser, database and special application software. Some of these vulnerabilities have led to loss or disclosure of data, unauthorised and embarrassing changes to websites, significant loss of access to network resources and large amounts of recovery effort.

Protection through latest software updates. Protection from exploitation of known security holes or bugs can be achieved by installing the latest software updates or patches to all servers and workstations. The School administration network is maintained and controlled by Central Office with the latest patches, anti-virus, etc. Although this process requires significant amounts of expertise and time, schools should also be vigilant and identify vulnerabilities and apply fixes to all non-centrally managed devices.

Patch updates. Wireless networks, connection of PDAs, smart phones, non-Department managed laptops, tablets and other devices all present a security risk to any school managed network if not patched and monitored diligently. For non-centrally managed devices, limited advice can be sought from your Customer Relationship Manager (CRM). Schools with networks that are not centrally managed should establish a relationship with their preferred panel integrator.

Monitor security. Those work sites that face a special risk, or have had a history of malicious activity, should appoint someone to monitor reports of security exposures discovered, together with the fixes that become available. That person should decide whether a particular fix addresses risks that have special significance for the particular site and liaise with the Customer Service Centre to determine appropriate ways of implementing updates ahead of the rest of the Department of Education.

Action

The network administrator should:

- *find out what version of the operating system software is on each server attached to the networks at the site;*
- *determine whether particular updates address risks of significance to the school; and*
- *maintain contact with other sources, such as the Customer Service Centre, in order to become aware of issues such as the reliability of software updates, precautions to take before installing updates, and plans for implementing updates across the Department.*

B.6. ANTI-MALWARE SOFTWARE

The damage caused by virus attacks and exploitation by other malware can lead to loss of access or destruction of computer-based data.

It is essential that all workstations and servers have the latest versions of anti-malware software. All administration devices have automatic update distribution processes in place that are managed centrally by the Customer Service Centre.

Non-centrally managed devices are not to be connected to the administration network. Schools should configure their non-centrally managed work stations to download updates daily. Seek advice from your preferred panel integrator should there be difficulties on any device in the school.

Action
The network administrator to check each month to ensure that automatic distribution processes for anti-virus and anti-malware software are working correctly.

B.7. APPLICATION SYSTEM SECURITY REQUIREMENTS

Some application systems have their own security sub-systems for restricting the access of users to different parts of the system. These systems include HRMIS, financial management systems, SIS and timetabling or other school management systems.

School ICT Coordinators should know what is needed to support the relevant systems. If instructions on how to manage the security of the applications are not available, they should be obtained from the vendors or installers.

It is important for someone at each site to know how the security requirements of different systems interact.

For operational or other reasons, the person administering a particular system may not be the School ICT Coordinator. In that case, the School ICT Coordinator should assist as best they can. They need to be alert to the risk of passwords being insecurely held on some systems and staff should be reminded of the risks of using the same password in different systems.

Action
The principal to confirm that the School ICT Coordinator knows as much as possible about the security arrangements of all application systems installed on the network.

B.8. SECURING EQUIPMENT

There are a number of risks to the information held on a network that can result from equipment mismanagement or neglect, including:

- theft of the server or computer holding the information;
- theft of backup tapes or disks;
- interference with equipment that has been left turned on and unattended;
- removal of equipment for maintenance or disposal (by donation or sale) that contains copies of sensitive information;
- use of non-secure methods for deleting old files, leaving them vulnerable to restoration by **UnDelete** or **UnErase** programs; and
- damage to equipment caused by environmental factors (such as dust, heat or humidity).

Schools are subjected to a significant number of security breaches and associated vandalism, arson and theft. The impact severely disrupts the normal daily routine of schools, adversely effects student outcomes, almost invariably places stress and tension on all the teachers and staff, and often results in the loss of valuable and irreplaceable personal resources, teaching materials and students' work, much of which is stored on network connected servers and computers.

Refer to the *School Security* policy for more information on protecting school equipment.

Secure lockable storage should be available for disks and backup tapes that are off-site. Backup tapes should be taken off-site and returned when required.

School ICT Coordinators should be alert to these issues and recommend to principals, measures to reduce security risks.

Staff involved in arranging for the maintenance or disposal of equipment are to check with their CRM for the availability of Department approved Secure Erasure software.

Action

The school principal should:

- *be familiar with the advice contained in the Schools Security Manual issued to each school.*
- *ensure that all staff involved in arranging the maintenance or disposal of equipment are aware of the need to properly remove sensitive information before doing so.*
- *only use reputable computer maintenance personnel who will respect your confidentiality requirements.*