Use of passwords

The security of some of our data is only as strong as the password used to protect it. When creating a password, try to make it as strong and unguessable as possible. In particular:

- Make it at least eight characters long
- Use numbers as well as upper and lower-case letters
- Use a passphrase rather than a word. For example, TheCatSatOnTheMat2020
- Don’t use publicly available information associated to you, such as your name, children’s names or date of birth
- Don’t use common passwords such as Password1 or 12345678
- Change your password if you think it has been compromised
- Never share your password with anyone else, including staff, third parties or even the [IT Support Desk]
- Don’t write your password down
- Use different passwords for different key systems where possible

This document

This document is intended to be a brief summary of some of the points set out within the set of [Leopard Imaging] information security policies. It is not comprehensive, and users are referred to a copy of the full policy documents which are available on the IT section of the intranet or upon request from the [IT Support Desk].

Secure use of email and defence against viruses

Users must be constantly vigilant against the threat of malicious code in the form of viruses. In order to minimize the risk of introducing a virus to the network, follow the following code of practice:

- Don’t open attachments unless you know they are from a reliable source
- Always scan files from outside the organization before storing them on the network
- Ensure your virus-scanning software is working correctly
- Always report any virus-related messages you encounter to the [IT Support Desk]
- Don’t download unauthorized software or files from the Interne

Leopard imaging

Information Security Policy Summary Card

- Passwords
- Email and viruses
- Staying secure when offsite

- Physical security
- Reporting a security incident
- Printing confidential information
- Transferring data outside the organization

Staying secure when offsite

Employees travelling on business are responsible for the security of information in their custody. They should not take confidential data offsite unless there is a valid reason to do so.

While offsite:

- Don’t leave laptops, tablets, phones or other portable IT equipment in an unattended vehicle
- Don’t advertise the fact that you have a device in your possession
- Use PINs and passwords to protect devices from unauthorized access

Physical security

When locating computers and other hardware, precautions are to be taken to guard against the environmental threats of fire, flood and excessive ambient temperature and humidity.

All employees should be aware of the need to challenge strangers on the organization’s premises. Consideration must be given to the secure storage of paper documentation containing sensitive or confidential information, such as customer files.

Reporting a security incident

All suspected information security incidents must be reported promptly to the Information Security Manager via the [IT Support Desk]. Provide the following information as a minimum:

- Name
- Department
- Contact Number
- Description of the incident
- Current and/or potential impact

Above all, think about what you are going to say and how will you explain your problem:

- Notify the [IT Support Desk] of any actual or potential breach of security immediately.
- Record any information which may help. For example, error messages
- Adhere to procedures when logging an incident
- Remain courteous to the people dealing with the incident
- Request escalation if required by following the appropriate procedure
- Adhere to policies and procedures relating to IT use, equipment maintenance and security
- Log out of the network and/or systems promptly when requested to do so

Printing confidential information

Confidential information should not be sent to an insecure, unattended printer where it may be seen or picked up by unauthorized people.

Where necessary, use PIN protection on multi-function devices.

Transferring data outside the organization

Where appropriate, sensitive or confidential information or data should always be transmitted in encrypted form.

Prior to sending information to third parties, not only must the intended recipient be authorized to receive such information, but the procedures and information security measures adopted by the third party must be seen to continue to assure the confidentiality and integrity of the information.

Never store confidential information in unauthorized cloud services.

If in doubt, contact the [IT Support Desk] for advice.