St Peter's College

Information Security Guidelines - Physical and Environmental Security

Procedures should be in place to ensure physical and environmental security.

To comply with the University's IS Policy you must:

1. Protect access to secure areas with entry controls
2. Define physical security perimeters
3. Implement protection against damage from natural or man-made disasters such as fire, flood, explosion etc
4. Protect critical infrastructure and resources from temporary losses of power or surges (UPS via College FroDo)
5. Ensure appropriate defence against intruders or unauthorized colleagues, using internal security software, eg varonis and firewall
6. Keep equipment hosting non-public data in secured areas
7. Protect media containing information from unauthorized access, misuse or corruption during transport beyond defined perimeters
8. Not take equipment off-site without prior authorization and appropriate risk assessment
9. Securely wipe any confidential data before equipment is sold on, transferred or disposed of (crushing of hard drives)
10. Implement revised Joiner and Leaver processes, including audit of master and other keys

Secure areas

Secure areas could be anything from a building or collection of buildings down to individual rooms or even particular devices. Defining 'security perimeters' therefore means ensuring all personnel are aware of who is authorised to access the area and who is not. This is usually done using signs such as 'staff only' and in general communication of policies to all personnel. For example there may be a local policy to ensure that only system administrators as allowed access to machine rooms, whereas other 'staff-only' areas may allow visitors to enter if they are signed in and wear appropriate identification.

In both cases however the policy should be clearly communicated to all staff/students and there should be signs and physical security controls (eg locked doors) in order to enforce the policy. All personnel should be made aware of who is authorised to access specific areas and should be encouraged to challenge and/or report any persons they come across who are suspected as being unauthorised. This may mean ensuring that authorised personnel wear visible identification at all times. Of course in certain circumstances this may not be possible or deemed appropriate and this should be determined by an assessment of the risk.

Appropriate physical security controls will depend on the nature of the secure area being protected. For example a server room may be classed as highly secure and require door locks, systems to record entry of individuals, CCTV and intruder detection. Alternatively areas accessible to College members only may simply require identification at the point of entry e.g. via a manned reception or SALTO type entry system. It may also be considered to protect certain individual machines from

theft or unauthorised physical access. This could be physically secured boxes or simply disabling external ports such as USB ports.

Appropriate physical security controls for offices will, again, depend on the specific environment and risk. However usually offices should be locked and only specifically authorised personnel given keys. All users should be made aware of who does have access to given office areas (e.g. cleaners, security staff) so that a judgement can be made as to how best to secure access to information within the office. For example, a clear desk policy may be desirable or a policy to keep sensitive information in locked drawers or safes. Using password protected screens or logging out of/switching off computers when leaving an office for a significant period should usually be encouraged as these are fairly cheap controls that will provide some mitigation against casual, opportunist or accidental breaches of data. In certain areas (e.g. open plan offices) screen locking etc may be particularly relevant.

Physical and environmental protection

The risk of natural or man-made disasters such as fires or floods should also be assessed before deciding where to site equipment, particularly if it is critical to the operation of the College. The frequency of flooding in the past, for example, can be used to help with such risks assessments. Where the risk is substantial, appropriate protection should be offered. This could be providing other, failover systems to introduce redundancy, physical protection, or deciding on alternative locations. Systems should also have proper ventilation if in areas that reach high temperatures such as switches in lofts or offices that get especially hot during the summer season. Adequate fans on systems in these situations are essential, including periodic reviews to ensure.

An Uninterruptable Power Supply (UPS) should be used for systems that require high availability, such as for core infrastructure including file servers and network equipment to protect them from failures in supporting utilities. Power line surge protection equipment should be used where UPS is not used, as these can help protect systems from damage from power irregularities. Redundant power supplies for critical systems should be considered to reduce the risk of downtime should a power supply fail, and can also provide ease of system power management such as connecting to a different UPS without causing system downtime.

Locations of power and network cables should documented and installed, where possible, along areas less likely to be affected by future construction projects, normal traffic by people or vehicles, heavy runoffs from roads and grit/snow removal equipment. As with systems, cables providing infrastructure support should not be exposed and accessible to passers-by, especially not in public areas. Installing cabling within walls, ceilings, or within covered trunking and out of easy reach can help reduce tampering and the possibility of intercepted network traffic or loss of service. Power and network port monitoring can be used to alert appropriate personnel if there is a change of state to any connected cables, providing a means of detecting any unauthorized interception or disconnection attempts.

Critical infrastructure equipment should have emergency contact details on it so the appropriate personnel are notified in the event of damage to the equipment or surrounding environment.

Off-site equipment and disposal

It is important that authorisation is received before taking equipment or information off-site. Such authorisation should be gained via the information asset owner and/or a line manager. The specific terms and conditions with which the information/equipment can be used off-site should be explicitly defined. For example, it may be strictly forbidden to make copies of certain data, use software on personal machines or allow others to use specific equipment. It may also be a condition to keep any portable devices such as USB sticks in locked rooms, drawers or cases to prevent accidental loss or theft. The use of encryption should be considered in addition when taking data off-site - see the InfoSec's 'Protect My Computer: Encrypt laptops and other portable devices' (https://www.infosec.ox.ac.uk/protect-my-computer.) Procedures should exist to ensure that any sensitive data and licensed software have been securely overwritten when equipment is transferred within the College and removed when equipment is sold on or recycled.