ST PETER'S COLLEGE
UNIVERSITY OF OXFORD

Information Security Guidelines - Incident Response

St. Peter's College is responsible for responding to information security incidents in a timely manner and for following the advice and guidance given by OxCERT and the Infosec team. Breaches of information security, including potential data breaches, should be reported to the information security team. Known data breaches should be reported immediately to the College Data Protection Officer.

St. Peter's College must:

1. Ensure information security incidents and potential data breaches are reported to infosec@it.ox.ac.uk
2. Report known breaches of the GDPR to dataprotection@spc.ox.ac.uk
3. Ensure computer and/or network security incidents are reported to OxCERT
4. Ensure responsibilities for reporting security events and incidents are defined and communicated to relevant personnel
5. Ensure suspected information security incidents are reported to a designated person or group
6. Ensure vulnerabilities or suspected weaknesses are reported to a designated person or group
7. Ensure that the types, volumes and costs of information security incidents can be quantified and measured
8. Have appropriate contingency plans for responding to security incidents
9. Have designated contacts for security incidents and ensure they are monitored during working hours irrespective of staff leave/absence
10. Respond to Infosec and OxCERT request within 4 working hours
11. Ensure necessary documentation can be made available to IT Services if required to investigate incidents that may impact on other parts of the University network
12. Ensure abusive or malicious traffic can be traced in accordance with OxCERT's Logging of network access page
13. Observe the University's guidelines when dealing with potentially illegal material
14. Be familiar with and follow OxCERT's Incident handling page for handling other computer and/or network security incidents

Incident Handling

In response to compromised machines, JICTS will usually impose a router level block. However, the compromised machine will still have local network access and it is in the interest of the College to isolate the machine as quickly as possible. Failure to do so may result in other compromised machines on the network and escalation of the incident. There have been several incidents where a large number of compromised machines have resulted in a college having their network connection temporarily suspended in order to contain and deal with the incident. Where OxCERT cannot impose a block on individual machines, colleges are expected to respond within 4 working hours

Colleges should ensure they have sufficient contingency plans in place for dealing with security incidents, including plans for rebuilding machines in the event of a system compromise. In many cases, where attackers have gained administrator privileges and/or there is insufficient logging there may be no alternative but to re-install systems from scratch. Colleges should take this into account when carrying out risk assessments on business-critical systems and when implementing redundancy. Care should be taken to avoid backup systems being open to the same vulnerability as the primary system (for example both using the same administrator password)