Procedure - Handling reports of misuse of IT (SaNS)

Team members of IS technical teams must not initiate any investigation of suspected IT misuse without involving a team manager.

The SaNS Manager (acting in the capacity of IT Security Officer) can become aware of the possibility of misuse of IT facilities by users in a variety of ways, including:

- SaNS staff may report dubious activity identified in the course of their routine work e.g. inappropriate use of filestore found when investigating unusual disk utilisation problems, loss of network service to a number of users owing to the unauthorised connection to the network of a "rogue" device.
- users' line managers may request information about an individual's use of IT facilities where they suspect inappropriate activity.
- users or security staff may report suspected inappropriate activity which they have observed in a Public space, such as an IT Lab. This may take the form of a formal complaint in which case action must be taken by IS, leading to a formal response.

Investigation of such reports or allegations is constrained by the following University Policies and Regulations, Legislation, and guidance from professional organisations:

- IS Regulations
- University IT Use Policy
- Regulation of Investigatory Powers Act
- Human Rights Act
- HEIDS / JISC Legal Inappropriate Use Investigation Process
- UCISA Exploiting and Protecting the Network, Institutional Policy and Practice

On becoming aware of potential misuse the SaNS Manager will initiate only as much investigation as is necessary to establish whether or not inappropriate activity has taken place. If, on reasonable investigation, no evidence of misuse is found then this will be reported, as appropriate, and no further action will be taken.

If evidence of a minor infringement is found the SaNS Manager will:

- contact the user to inform them that there is evidence that they have misused University IT facilities
- draw the user's attention to the relevant regulation
- request that the user take action to remedy the situation
- advise the user not to repeat the offence
- inform the user that further misuse on their part may be reported to the Director of Information Services and may result in disciplinary action against them

If there is evidence of more serious misuse the SaNS Manager will report this to the Director of IS and advise the Director on the desirability of the following actions:

- disciplinary action against the user
- suspension of IT facilities pending further investigation
- involving the Police

Further investigation will only be performed under instruction and with authorisation as per the constraints described above. Those who instruct/authorise the investigation will inform the user under investigation about the process to the extent that they deem necessary.

The SaNS Manager may involve members of other IS technical teams in the investigation as necessary. Detailed records will be kept by the SaNS Manager as to equipment and data scrutinised, findings, and conclusions. At the conclusion of the investigation a written report will be provided to the Director of IS.

Alan Richardson
SaNS Manager

September 2013

Explanatory Notes

Logging, **Monitoring** and **Investigation**

Logging is merely data gathering so that evidence is available if it is required. The information that is gathered is only scrutinised when a reason to do so arises. Logs are continuously generated for most IT systems to varying degrees, and Information Services has a log retention Policy.

Monitoring is routine inspection of data gathered by logging, usually with the intention of identifying inappropriate behaviour so that proactive action can be taken to stop that behaviour. Monitoring is not performed at Stirling University, though dubious behaviour sometimes becomes apparent when a subset of logs are being scrutinised in order to solve a particular problem; indeed the problem may have been caused by the inappropriate behaviour. That accidental discovery may occur is acceptable, but scrutiny must stop as soon as a suspicion arises, until further investigation is authorised by a manager.

Investigation is taking place when a log is being analysed with the specific purpose of determining whether an inappropriate activity has taken place i.e. specific evidence is being sought to prove (or disprove by absence of evidence) a particular case. That action must not be taken without consulting a manager. Mechanisms for collecting information (actions 1-4 below) may be initiated providing the logs produced are not subsequently analysed without authorisation.

A team member may, on their own initiative start or modify logging processes in order to collect evidence in a timely fashion. Such activities include:
1) increasing a log verbosity level
2) starting a network packet trace of traffic involving a particular client system on the network
3) retaining specific backup media for longer than normal
4) taking a special backup or copy of user data including a home directory or email mailbox

The SaNS Manager should be informed that such a process has been initiated, and the reason for it.

In the absence of the SaNS Manager, alternative management advice may be sought from the manager of ITCS, the manager of BSDS, or the Director of IS.

When a suspicion of possible misuse arises during the course of work intended to solve a previously identified IT problem, that work may continue only to the extent necessary to resolve the original issue. If further evidence is inadvertently uncovered as a result of that work this will not be construed as "investigation". Reasonable efforts should be made in the course of the work not to modify or destroy any data which may constitute evidence of misuse.

If misuse is suspected that would be significantly detrimental to the University if allowed to continue, e.g. the sending of spam messages to third parties, large scale blocking of legitimate network communications by a "rogue" device, SaNS staff may (immediately, without the approval of a manager) take measures which will reduce the impact of the misuse but which do not disadvantage the owner of the account being used, i.e. block outbound emails from that account or disable the network port the offending device is on, but do not prevent the user from making legitimate use of IT services (for example by locking their network account).