University of Sheffield Code of Connection

You are responsible for the activities and security of your user account and any systems you have connected to, or registered on, the University network.

If you are running a service (e.g. a website) from that system then there are additional risks and responsibilities that you must be aware of:

- **Governance** - You must comply with the University's IT Code of Practice and any other relevant policies and procedures. - www.shef.ac.uk/cics/codeofpractice

- **Records -** You must keep records of ownership up to date. If you fail to keep the record up to date and we are unable to contact the current owner then systems may be disconnected from the network. - www.shef.ac.uk/cics/forms

- **Patching** - Security patches must be applied promptly. Unpatched systems may be suspended from the University network.

- **Antivirus software** - All systems which are able to do so should have antivirus installed, enabled, updated and configured appropriately.

- **Firewall** - All systems which are able to do so should have a firewall installed, enabled and configured appropriately. www.shef.ac.uk/cics/firewall

- **Secure development -** If providing a service or application (e.g. a web application) then you must ensure that the system has been developed in accordance with recognised good security practice. We recommend the following introductory guides and standards as a starting point:
  - https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf
  - https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

- **Security testing** - CiCS tests the security of systems connected to the University network. You must not carry out any unauthorised security tests (e.g. vulnerability testing of other peoples systems). You can request a security test of your system or application by contacting ipreg@sheffield.ac.uk

- **IT Security** - Systems should be secured/hardened in accordance with vendor supplied and/or industry good practice guides. Systems communicating sensitive information should only do so over secure protocols such as SSH/HTTPS. Unused/insecure network services must be disabled.

- **Accounts and passwords** - Only necessary accounts should be enabled; unused accounts and guest accounts should be disabled. All accounts must be protected with strong passwords. Default usernames and passwords must be changed.

- **Network management** - You must not extend the University network (for example by using a wireless access point) without authorisation.

- **PCI DSS -** Any technology involved in the storage, transmission or processing of debit/credit card information or that can potentially impact on the security of the cardholder environment must adhere to the University of Sheffield PCI DSS Information Security Standard.

- **Security Incidents -** You must report all security incidents to CiCS in accordance with the University's Information Security Incident Policy - www.shef.ac.uk/cics/infosec

If you have any questions about the above points or require advice on configuring and securing your system then please contact ipreg@sheffield.ac.uk