Cyber Essentials Assured Computing Policy

This document is uncontrolled when printed.
Before use, check to verify that this is the current version.
Compliance is mandatory.

Version and Ownership

Version	Date	Author(s)	Comments
0.01	02/05/2017	Chris Willis - Information Security Manager	Draft
1.00	10/08/2017	Geoff Kendall-Smith - Director of CiCS	Approved v1.0
1.5	07/11/2018	Sinead O'Brien - Information Security Compliance Officer	Minor Revisions
2.00	18/11/2018	Jon McAuley Interim Director	Approved v2.0

Overview

This policy defines a set of Cyber Essentials certified research IT services at the University of Sheffield. This policy also includes the key policy statements and working practices required to ensure compliance to the Cyber Essentials standard.

Purpose

The policy allows researchers to take advantage of Cyber Essentials certified systems and processes; this enables safe working and the ability to work on projects where the use of Cyber Essentials compliant IT services is a prerequisite.

Scope

This policy applies to the following IT services provided by the University's IT department, Corporate Information and Computing Services (CiCS):

- The Managed Desktop service - https://www.shef.ac.uk/cics/desktop
    - This is a fully managed desktop solution, users have no privileged access. All critical security controls are managed by CiCS.
- The YoYo Desktop service - https://www.shef.ac.uk/cics/yoyo-desktop/introducing-yoyo-desktop
    - This is an enrolled desktop solution, users can request privileged accounts in order to install essential applications. Privileged accounts are separate to a user's normal account and must not be used for day-to-day activities. All critical security controls are managed by CiCS.
- Research Virtual machines - https://www.shef.ac.uk/cics/research/infrastructure
    - These are Windows/Linux based virtual machines. Users are given privileged accounts so that they can install essential applications. All critical security controls are managed by CiCS.
- Research Data Storage - https://www.sheffield.ac.uk/cics/research-storage
    - Networked storage provided to researchers and available via the above compute services. All critical security controls are managed by CiCS.
- GSuite for Education - https://www.shef.ac.uk/cics/google
    - Google applications provided to the University, this includes email, collaborative filestore and calendar. Critical security controls are maintained by Google (with CiCS managing the configuration of controls where appropriate).
- Infrastructure supporting the above services (e.g. networking, servers, authentication services, storage)
    - All critical security controls are managed by CiCS.

This policy applies to users of the above services (who want to take advantage of the Cyber Essentials certification) and those responsible for the administration and support of the above services.

Policy

"To ensure that your data is being processed in a Cyber Essentials certified environment then you must comply with the Cyber Essentials standard and the instructions provided by CiCS"

By using the certified Cyber Essentials Assured Computing service and applicable processes you will have assurance that you are working in a Cyber Essentials secure environment.

As administrators of the service CiCS will ensure that the storage and compute services described above remain compliant and adhere to the requirements of Cyber Essentials[1].

All users of the services must ensure that:

- They complete the short online training course **Training for Cyber Essentials Assured Computing**
- Data is stored on the Research Data Storage service or Google Drive.
- Data is only accessed and processed on the Managed Desktop, YoYo Desktop or Research Virtual Machine services.
- They do not circumvent any of the security controls put in place by CiCS. For example, disabling firewalls, anti-virus, automated patching.
- Software must only be installed from trusted sources.
- If you install software from anywhere other than the University of Sheffield Software Centre you are responsible for keeping that software up to date at all times.

The YoYo Desktop and Research Virtual Machine services allow privileged accounts. These accounts are able to access the internet so that essential applications (e.g. to support research) and patches can be installed. These accounts must not be used for any purpose other than the administration of the system.

Any data accessed or taken outside of the certified Cyber Essentials Assured Computing service(e.g. printed out, copied onto a personal laptop, phone, memory stick or personal cloud account) will no longer be assured to Cyber Essentials.

Policy Compliance

The University's Information Security team will annually review the status of the certified Cyber Essentials Assured Computing service. The University's Information Security team will maintain the Cyber Essentials certification.
Any breach of policy must be reported as an Information Security Incident - https://www.shef.ac.uk/cics/policies/securityincident

Related Standards, Policies and Processes

The University's Information Security Policies - https://www.shef.ac.uk/cics/infosec
The University's IT Code of Practice - https://www.shef.ac.uk/cics/codeofpractice
The University's assessment of the security of Google Apps - https://www.shef.ac.uk/cics/google/security

[1] https://www.cyberaware.gov.uk/cyberessentials/files/requirements.pdf