Security Overview

Version 1.13

Created date:	26 January 2012
Last updated:	09 March 2018
Review Due:	24 August 2018
Authors:	Tony Austin, Tim Evans, Ray Moore and Paul Young
Maintained by:	Digital Archivists, Systems Administrator & Software Developer, Communications and Access Manager
Previous version:	Version 1.12

Security Overview

Security is of primary importance at multiple levels. All of the below is based on the official University of York IT Services Security.[1]

Basic PC security

Centrally managed (supported) machines

PCs have strong security measures in place including the deployment of anti-virus software and malware protection (McAfee Endpoint Protection). A series of centrally managed platform specific firewalls are utilised throughout the network (Windows Firewall, Apple OS X, Ubuntu UFW, etc). Some useful web pages include:

- IT Services security overview[1]
- IT Services general information about IT Accounts[2] (managed through *York Identity Manager)*
- IT Services anti-virus software[3]
- IT Services network settings and firewall[4]
- IT Services spam and phishing emails advice[5]
- IT Services password management[6]

[1] https://www.york.ac.uk/it-services/security/

[2] https://www.york.ac.uk/it-services/accounts/

[3] https://www.york.ac.uk/it-services/security/virus/

[4] https://www.york.ac.uk/it-services/security/network/

[5] https://www.york.ac.uk/it-services/security/spam/

[6] https://www.york.ac.uk/it-services/security/password/

Unsupported machines including home computers

Where possible users are advised to make sure they have the same sort of services available as described for supported machines.

Modern computer systems usually have bundled firewalls, but they may need to be activated.

If an unsupported machine does not have anti-virus software, McAfee can be downloaded under agreement from the University.[7]

Other measures

- PC passwords have to be changed every 365 days via York Identity Manager[8]
- Use strong passwords[9] and follow the password policy.[10]
- Passwords should never be written down. The use of password managers allow the secure storage store of login credentials, including usernames and passwords. The University provides recommendations on password managers.[11]
- PCs should be locked when left unattended.[12]
- Make sure the operating system and software is up-to-date[13]
- Virus and malware software should be installed and run regularly.[14]
- Consider using script blocking software, such as the Mozilla-based browser extension *NoScript*[15], the Chrome-based *ScriptSafe*[16], etc
- External media (i.e. portable drives and disks including those in portable computers) that are also used outside the University firewall can be a major threat to security. Infections picked up outside can be moved into the University's protective environment. It thus makes sense to scan such media coming into the University environment. This should happen automatically if your anti-virus software is set up correctly. The university provides guidance on protecting confidential information through the use of encryption[17], with further guidance on the safe sharing of data and cloud services.[18]

Data storage

Recovery can only happen if data is backed up. Various options exist for ensuring backup

- Personal filestore: On supported machines multiple snapshots (hourly, nightly and weekly) are taken of your M: and H: drives.[19] Clearly this is the securest place in terms of backup to keep important data/documents but space is limited. Guidance on restoring data is also provided.[20]

[7] https://www.york.ac.uk/it-services/security/virus/
[8] https://www.york.ac.uk/it-services/security/password/
[9] https://www.york.ac.uk/it-services/security/password/strong/
[10] https://www.york.ac.uk/it-services/security/password/policychanges/
[11] https://www.york.ac.uk/it-services/security/password/managing/
[12] https://www.york.ac.uk/it-services/security/screen-lock/
[13] https://www.york.ac.uk/it-services/security/update/
[14] https://www.york.ac.uk/it-services/security/virus/
[15] https://noscript.net/
[16] https://chrome.google.com/webstore/detail/scriptsafe/
[17] https://www.york.ac.uk/it-services/security/encryption/
[18] https://www.york.ac.uk/it-services/security/dropbox/
[19] https://www.york.ac.uk/it-services/filestore/
[20] https://www.york.ac.uk/it-services/services/backups/

- Personal Google Drive: Data can also be saved to a personal Google Drive.[21]
- Shared filestore: For use of groups or projects where centralised access to information is necessary.[22]
- Shared Google Drive.[23]

Data sharing

IT Services provide a number of sharing serves through which data can be sent or received.

- Google Drive[24]
- University of York DropOff Service[25]
- File transfer (SFTP and SCP)[26]

ADS Offices

Generally security services within the University of York are provided by the university Security Services[27], with a dedicated Service Level Agreement and surveillance policy.[28] The ADS offices are situated in the Department of Archaeology at The King's Manor in York.[29] As an important historic building in York, parts of The King's Manor are open to the public during working hours and at weekends, however, specific access to the ADS offices is restricted by key, key card and keypad security systems.[30] An on-site security team also routinely monitor access to the buildings at King's Manor utilising the dedicated CCTV systems. Out of office hours the King's Manor is subject to intruder alarms, CCTV systems and routine security sweeps.

The ADS adheres to the University of York general policies concerning members of staff who leave the organisation[31], with a further policy on access to electronic resources.[32] Specific security issues to the ADS offices are managed and addressed by the ADS Administrator.

ADS Systems Security

As part of the University of York the ADS adheres to the official policies and guidelines set out above, but at the same time takes steps to secure its own data. The ADS follows the guidelines laid out in the University of York's summarised above, with additional security outlined below:

[21] https://www.york.ac.uk/it-services/services/drive/

[22] https://www.york.ac.uk/it-services/filestore/rented/

[23] https://www.york.ac.uk/it-services/services/drive/

[24] https://www.york.ac.uk/it-services/services/drive/

[25] https://www.york.ac.uk/it-services/services/dropoff/

[26] https://www.york.ac.uk/it-services/services/file-transfer/

[27] https://www.york.ac.uk/admin/security/index.html

[28] https://www.york.ac.uk/admin/security/service-level-agreement/v%202.0%20Section%20Service%20Level%20Agreement%20April%202014.docx and https://www.york.ac.uk/admin/security/statistics/

[29] https://www.york.ac.uk/about/campus/landmarks/kings-manor/

[30] https://www.york.ac.uk/admin/security/access-control/

[31] https://www.york.ac.uk/admin/hr/contracts-and-appointments/leaving-the-university/resigning/

[32] https://www.york.ac.uk/it-services/accounts/staff-leavers/

Passwords

- Password management: all passwords for ADS systems are encrypted and stored in a centrally managed Password Management system.
- Unique passwords are created for each domain, file store and applications.
- Passwords are updated regularly, typically every 6 months, via the Password Management system.
- Passwords are shared to individual members of staff, relevant to their needs and working practices.

When members of staff changes role or leave the organisation, the ADS adheres to the guidelines outlined by the University of York IT Service.[33] Internal ADS passwords are changed, updated or removed as appropriate within the Password Management system.

Systems Access

- Systems and applications are mounted on discrete independent virtual servers to improve security and reduce interdependence.
- Discrete levels of access are provided for each user appropriate to their working needs.

When members of staff changes role or leave the organisation, the ADS adheres to the guidelines outlined by the University of York IT Service.[34] Access to ADS systems and resources are password controlled (see above for discussion of passwords).

Data storage

- Shared filestore: ADS (and *Internet Archaeology*[35]) staff have access to a shared 'backup' drive which can be mapped to their supported PCs. This drive is backed up nightly by IT Services.[36]
- Local data storage: As outlined in the Preservation Policy the ADS maintains multiple copies of data to facilitation disaster recovery. All data is maintained on a centralised server maintained by the University of York IT Services. They are backed up to tape and maintained off site. Currently this system uses Legato Networker and an Adic Scalar tape library. This involves daily (overnight), weekly and monthly backups to a fixed number of media so tapes are recycled.[37]
- Off site data storage (Essex): Data is synchronised once a week from the local copy in the University of York to a dedicated off-site store maintained by the UK Data Archive at the University of Essex.[38] This repository takes the form of a standalone server (see SLA) behind the University of Essex firewall. Data is further backed up to tape by the UKDA (see UKDA Preservation Policy).[39]

[33] https://www.york.ac.uk/it-services/accounts/staff-leavers/

[34] https://www.york.ac.uk/it-services/accounts/staff-leavers/

[35] http://intarch.ac.uk/

[36] https://www.york.ac.uk/it-services/filestore/rented/

[37] For further discussion see the *Preservation Policy* - http://archaeologydataservice.ac.uk/advice/PreservationPolicyRev.xhtml

[38] http://www.data-archive.ac.uk/

[39] For further discussion see the *Preservation Policy* - http://archaeologydataservice.ac.uk/advice/PreservationPolicyRev.xhtml

When members of staff changes role or leave the organisation, access to university storage is removed (see guidelines outlined by the University of York IT Service)[40] and access to the stored data, ADS systems and resources is similarly removed.

Data sharing (with the ADS)

- Physical media: The ADS often receives data sent on a variety of physical media via the postal or courier services. Care is taken on receipt to follow the guidelines on security provided by the University of York IT Services.[41] At the same time the ADS follows its own protocols on checking deposition data. These can be found in the *ADS Ingest Manual.*[42]
- ADS-easy: The ADS' own system of digital submission system, ADS-easy[43], allows users to create metadata and upload data directly to the ADS servers. Protocols are in place to make sure that data sent in this manner adhere to the guidelines set out by the University of York IT Services[44], and are outlined in the *ADS Ingest Manual*.[45]
- Digital exchange: Where data is exchanged outside of the ADS-easy system, through Google Drive, University of York DropOff Service, or other file sharing services (e.g. DropBox, OneDrive, etc) the ADS follows the guidelines on security provided by the University of York IT Services.[46] In either case the ADS follows its own protocols on the deposition of data into the archive which are outlined in the *ADS Ingest Manual*.[47]

Data sharing (with users)

- ADS website: Generally all data from the Dissemination Information Package (DIP) of each archive is accessible through the ADS website. In some circumstances, where the data set is large, these may be arranged in a series of multi-zip files, see for example the *Butser Ancient Farm Project Archive 1972-2007*.[48] Note that these have been created in compliance with the University of York IT Services security guidelines.[49]
- Physical media or Digital exchange: In a few circumstances, where datasets are too large for dissemination through the ADS website, these are made available on a 'on request' basis through the exchange of physical media or data exchange services. In either case, compliance to the University of York IT Services security guidelines is mandated.[50]

The access policy for ADS resources is outlined in the Preservation Policy[51], the Sensitive Data Policy[52] and the ADS' Terms and Conditions.[53] In a small number of cases access to data may be restricted or embargoed at the request of depositors. Typically such restrictions are short term and are negotiated on a case by case basis.

[40] https://www.york.ac.uk/it-services/accounts/staff-leavers/
[41] https://www.york.ac.uk/it-services/security/
[42] http://archaeologydataservice.ac.uk/advice/Ingest.xhtml
[43] http://archaeologydataservice.ac.uk/easy/
[44] https://www.york.ac.uk/it-services/security/
[45] http://archaeologydataservice.ac.uk/advice/Ingest.xhtml
[46] https://www.york.ac.uk/it-services/security/
[47] http://archaeologydataservice.ac.uk/advice/Ingest.xhtml
[48] http://archaeologydataservice.ac.uk/archives/view/butser_baf_2016/downloads.cfm?archive=video
[49] https://www.york.ac.uk/it-services/security/
[50] https://www.york.ac.uk/it-services/security/
[51] http://archaeologydataservice.ac.uk/advice/PreservationPolicyRev.xhtml
[52] http://archaeologydataservice.ac.uk/advice/sensitiveDataPolicy.xhtml
[53] http://archaeologydataservice.ac.uk/advice/WebsiteTerms.xhtml

Personal data

A small number of ADS services require users to register for access, e.g. OASIS, ADS-easy, etc., and provide information about themselves. Where personal data is held, the ADS recognises the importance of personal privacy and ensures that all personal data is held in accordance with the Data Protection Act 1998. Compliance is managed in accordance with the University of York's Data Protection Act[54] and the ADS' Privacy Policy.[55] We are currently working to bring out systems in line with the EU's General Data Protection Regulation (GDPR) which comes into effect in May 2018.[56] In those circumstances where users register for services, all passwords are stored in a hashed form.

The personal information of depositors, such as telephone, email and postal addresses, etc. may also be stored within the ADS' Collection's Management System. In these circumstances, the ADS ensures that personal data is stored in accordance with the Data Protection Act 1998. Compliance is managed in accordance with the University of York's Data Protection Act.[57]

The ADS also uses Matomo Web Analytics for the purposes of collecting statistics about website usage for which some non-personally-identifying information may be collected, alongside widgets from social media websites. A full list can be found in the cookies policy document.[58]

[54] https://www.york.ac.uk/records-management/dp/
[55] http://archaeologydataservice.ac.uk/advice/Privacy.xhtml
[56] https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation
[57] https://www.york.ac.uk/records-management/dp/
[58] http://archaeologydataservice.ac.uk/about/Cookies.xhtml