Data Security Protection Toolkit Information Security Policy

Document Information	
Author	Information Security Officer (Technical)
Version	6.0
Date Approved	24th June 2022
Approved By	FMS Information Governance for Health Research Group

Document History		
Version	**Date**	**Summary of Change**
1.1	08/10/2015	Section5 Access to Assets (project specific)
1.1	08/10/2015	Section 9 Encryption clarification on backups added
1.1	09/10/2015	Section13 includes network firewall standard
1.1	08/10/2015	Section 14 Hardcopy asset destruction
1.2	13/10/2015	Section 14 Hardcopy asset destruction clarification
1.3	10/06/2016	Section 9. Encryption updated AES 256
1.3	10/06/2016	Section 5. Access to Assets clarification added.
1.3	14/06/2016	Section 6. Clarification on Backups and Disaster recovery added
1.3	14/06/2016	Section 14 Data Destruction amended to include time periods and encryption Keys
1.3	13/07/2016	Section 6 Further details on backup locations added.
1.4	11/08/2016	Details on Third party included and connection type.
1.5	21/10/2016	Rebranding Document for use for IGT
1.5	21/10/2016	Updated Technical descriptions to match with Technical Implementation.
2.0	14/07/2017	No changes required.
3.0	01/05/2018	Change reference to DSPT, and GDPR
4.0		Appendix D updated to reflect changes in Infrastructure
5.0	20/05/2021	Change of FMS IGHR
6.0	09/06/2022	Appendix D updated to reflect changes in Infrastructure

DSPT Information Security Policy

1. Scope

This Local Information Security Policy mandates controls to safeguard the confidentiality, integrity and/or availability for all **ASSETS** documented in the Information Asset Inventory declared in the Toolkit Enrolment documents; and the restricted access **WORK ENVIRONMENT** these are the locations declared in the Toolkit Enrolment documents.

This policy applies to all personnel who access **ASSETS** within the **WORK ENVIRONMENT**.

The **CORRECT AUTHORITY** refers to the local information risk owners who are declared in the Toolkit Enrolment documents.

2. User Education & Awareness

All personnel who access **ASSETS** **MUST** complete information governance training and attend the IG induction session that covers:

- Acceptable use and safeguarding of **ASSETS**.
- Data incident reporting.

3. Physical Security

ASSETS **MUST** only be collected, stored and/or processed in a **WORK ENVIRONMENT** that is protected by the following physical security controls:

- Doors and windows that can be securely closed.
- Intruder alarm and CCTV that monitors the building perimeter and points of entry.
- Building fabric that prevents unauthorised access *(e.g. through artificial ceilings and flooring, and ducts used for ventilation, cabling and piping, etc.)*.

Only personnel authorised by the **CORRECT AUTHORITY** can access the **WORK ENVIRONMENT**. All personnel inside the **WORK ENVIRONMENT**:

- **MUST** wear visible University photo ID at all times.
- **MUST** not allow anyone to tailgate during entry.
- **MUST** ensure all doors and windows are securely closed when unattended.
- **MUST** immediately report all weaknesses in physical security that could result in unauthorised access to Estates Services.

Visitors to the **WORK ENVIRONMENT**:

- **MUST** sign-in and out at the designated reception area.
- **MUST** be supervised at all times upon entry.

4. Accessing the Network

Computer users within the **WORK ENVIRONMENT**:

- **MUST** be assigned a unique username and password.
- **MUST** log on in the context of a standard user; unless there is a valid formally documented business case authorised by the **CORRECT AUTHORITY** for administrator/root level access; if this is the case, then all administrative access **MUST** be through an administrator/root account that is unique to each user.
- **MUST** use “sudo” or “run as” when performing administrator/root level system operations.
- **MUST** be prevented from accessing IT Services without a valid username and password.
- **MUST** not allow anybody else to use their user account.

- **MUST** use a complex password as described by the IT Service here.
- **MUST** keep their password secret at all times.
- **MUST** not disclose their password in response to any communication claiming to come from the IT Service, or any other party *(e.g. social engineering, phishing, pharming)*.
- **MUST** immediately notify the Cyber Security Team if they believe their user account or password has been compromised

5. Access to Assets

Electronic **ASSETS MUST** only be accessed from computers physically located in the **WORK ENVIRONMENT** and have been hardened in accordance with section 12; unless there is a valid and formally documented business case that is authorised by the **CORRECT AUTHORITY** to access **ASSETS** from computers at other locations. Approval must only be given where assurances are sort that these devices meet the requirements as per section 9, 10 and 12 of this policy.

Access to electronic **ASSETS MUST** be controlled using group-based permissions and access will only be granted after successfully completing the mandatory training and signed and returned the agreement form at the back of the DSPT Handbook. Where the toolkit is used for the purpose of securing data from NHS Digital, only users mentioned in the NHS Digital Data Sharing Agreement can be added to the group. All users who access **ASSETS MUST** be a toolkit member. Users **MUST** only be added to the group if there is a valid and formally documented business case that is authorised by the **CORRECT AUTHORITY** stating that the users have been added to the Data Sharing Agreement (In the case of the toolkit being used to access NHS Digital Data), and/or have been added to the toolkit member list. Users **MUST** be immediately removed from the group if they are no longer employed within the **WORK ENVIRONMENT**. Group permissions **MUST** be reviewed at any changes to the group.

Hardcopy **ASSETS MUST** not be removed from the **WORK ENVIRONMENT**; unless there is a valid formally documented business case that is authorised by the **CORRECT AUTHORITY** for taking **ASSETS** off-site.

Remote access to ASSETS are only permitted via the University WVD or via a University Laptop with Direct Access enabled.

ASSETS MUST not be accessed through a public Wi-Fi network;

6. Storing Electronic Assets

Electronic **ASSETS MUST** only be stored on the University dedicated project area and backed-up file-servers that are managed by the University's IT Service; unless there is a valid, formally documented, and authorised business case for storing **ASSETS** on other devices. Backups of **ASSETS** not stored in the project area must be kept completely separate from the primary storage area and must be kept in a secure area. Such as Fire proof safe in a different building to the primary data.

Technical details on the University secure technical solution can be found in Appendix D

7. Clear Screen & Desk

Computer users within the **WORK ENVIRONMENT**:

- **MUST** lock the computer if it is left unattended for a short period of time *(e.g. a lunch break, etc.).*
- **MUST** log-off the network if leaving for longer periods *(e.g. overnight, weekends, or annual leave etc.)*; unless there is a valid formally documented business case authorised by **the CORRECT AUTHORITY** for keeping a locked computer logged-on *(e.g. the automated processing of large research datasets, etc.)*.

Personnel who work with sensitive hardcopy **ASSETS**:

- **MUST** securely store unattended sensitive hardcopy **ASSETS** in a locked drawer or filing cabinet.
- **MUST** keep drawer and filing cabinet keys secure *(e.g. stored in a key safe when unattended)*.

8. Portable Computing & Storage Devices

ASSETS MUST not be collected, stored and/or processed on portable computing devices *(e.g., laptops, tablets, smartphones, smart watches, augmented reality visors, etc.)* or portable storage devices *(e.g. external HDDs, USB data sticks, SD cards, DVDs, CDs, etc.)*; unless there is a valid formally documented business case authorised by the **CORRECT AUTHORITY**; and appropriate encryption controls are used to safeguard the **ASSETS**.

9. Encryption

All electronic **ENDPOINTS MUST** be encrypted using secure non-proprietary encryption algorithms, such as AES (Advanced Encryption Standard) 128 bit or higher. Full disk encryption **MUST** be applied to all endpoints used to collect, store and/or process the data. Encryption products **MUST** be obtained from trusted sources.

Encryption keys/passwords:

- **MUST** be sufficiently strong enough to prevent successful brute force attacks.
- **MUST** not be disclosed to unauthorised persons.
- **MUST** be changed immediately if they are believed to be compromised.
- **MUST** never be stored with encrypted **ASSETS**.

The University's IT Service cannot recover encrypted **ASSETS** if encryption keys/passwords are lost. There **MUST** be an appointed **KEY/PASSWORD CUSTODIAN** *(Appendix C)* within the **WORK ENVIRONMENT** who is responsible for ensuring encryption keys/passwords can be recovered in the event of a disaster.

10. Viruses & Malicious Software

Microsoft Defender for Endpoint Anti-virus and anti-malware software:

- **MUST** be installed on all end-points used to collect, store and/or process the data.
- **MUST** be maintained at the vendor's latest engine and definition/signature release.
- **MUST have Realtime scanning enabled.**

All software installers:

- **MUST** be obtained from trusted sources.
- **MUST** be correctly licensed.
- **MUST** be approved by Cyber Security Team

11. End-User Messaging Technologies

ASSETS MUST not by transmitted using end-user messaging technologies, such as social media, University email, Teams, Sharepoint, Teams Chat and/or instant messaging.

12. Device Hardening

Devices used to collect, store and/or process **ASSETS MUST** be hardened in compliance with vendor security recommendations; and Newcastle University's Code of Connection. In summary devices:

- **MUST** have a BIOS password set.
- **MUST** be managed by the University IT Service refer to point 5 for any exceptions.
- **MUST** have the BIOS configured so that the HDD is the first boot device.

- **MUST** only be running software that is vendor supported.
- **MUST** be in receipt of the latest security updates for firmware, operating systems, all installed applications, and all installed middleware *(e.g. Java, Adobe Flash, etc.) within 14 calendar days*.
- **MUST** not run default configurations that can be used to compromise the security of the device *(e.g. default passwords, guest accounts, etc.).*
- **MUST** not run unnecessary services.
- **MUST** not run non-secure remote access protocols *(e.g. rlogin, rsh, telnet, ftp, etc.).*
- **MUST** have local event logging enabled.
- **MUST** not be able to boot from a device connected to a USB port.
- **MUST** have a designated threat protection client installed for monitoring purposes.
- **MUST** be scanned quarterly for software vulnerabilities.
- **MUST** be subject to an annual IT security health check**.**

13. Network Security

Devices used to collect, store and/or process **ASSETS:**

- **MUST** be situated behind the University's firewall which are Common Criteria EAL4 compliant.
- **MUST** be running local software firewalls that deny all untrusted inbound network connections.
- **MUST** be situated on a subnet that uses a private RFC1918 compliant IP address scheme.

14. Disposal of Data

ASSETS that are no longer needed **MUST** be destroyed using methods that render data recovery impossible within 14 days of either a deletion notice or the termination of the Data Sharing Agreement or Framework Contract:

- Key Custodian **MUST** destroy all copies of file level Encryption keys rendering any data recovery impossible.
- Electronic **ASSETS MUST** be destroyed in accordance with our WEEE disposal agreement, and a disposal certificate must be retained. The disposal methods comply with HMG Infosec Standard 5 (IS5).
- All hardcopy **ASSETS MUST** be destroyed using a DIN 66399 Level 4 cross-cut shredder on site and then collected and destroyed by the University's contracted data disposal company.

15. Security Incidents

Security incidents involving the **ASSETS MUST** be immediately reported to the Cyber Security Team through the IT Service Desk on Ext 85999

16. Compliance Monitoring and Auditing

All toolkit members will be monitored and audited for compliance to this policy. Auditing will take place in accordance with the Confidentiality Audit Process.

17. Breaches of Policy

Breaches of this policy may lead to; revoked access to **ASSETS**; revoked access to University IT Services; and/or disciplinary proceedings.

END OF POLICY

APPENDIX A Newcastle University Secure Technical Environment

NHS Approved Data Storage

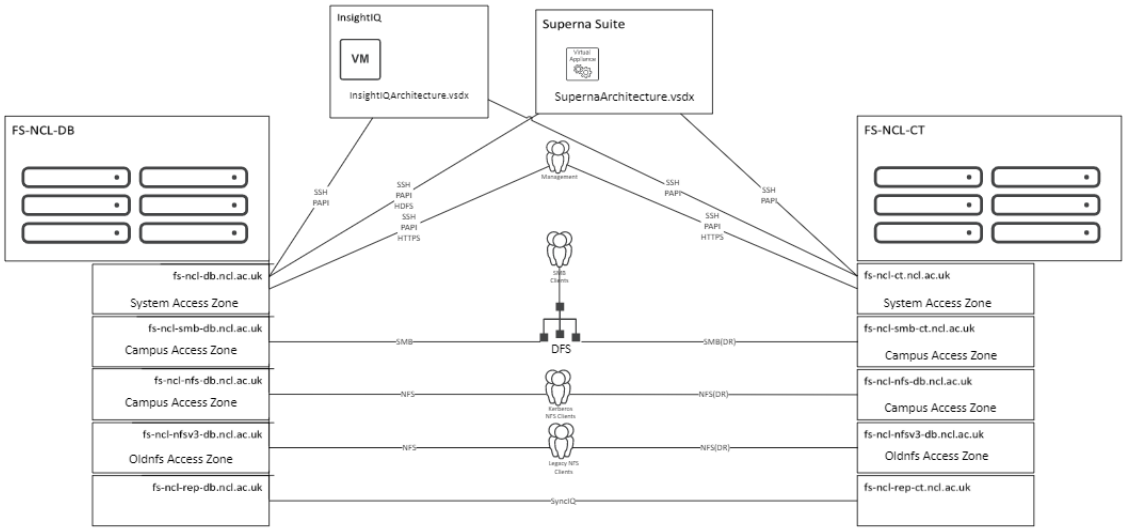
University Project Storage High Level Description

Project shares are located on the Isilon Clusters FS-NCL-DB and FS-NCL-CT. Each cluster consists of 8 H500 High Performance Nodes and 20 Capacity Nodes.

Project shares are stored within the RDW Section of the storage with Security regulated by groups with Read and Modify permissions. Superna Eyeglass, Easy Auditor and Search and Rescue are being used to find and recover misplaced data(Folders or files that have been accidentally moved to subfolders or other locations within Isilon), allow for Access Auditing and monitor and orchestrate Disaster Recovery, Business Continuity and Failover Aspects.

Additionally DellEMC InsightIQ is used to monitor cluster performance and health.

Server Setup



+

Security Permissions

Security permissions will be applied to the applicable folders and shares of the project. The security permissions make use of the groups in active directory. These groups can be managed by either through the normal active directory tools, or by using the service Grouper. Grouper provides the ability to update groups within active directory using an easy to use interface, https://groups.ncl.ac.uk.

Only the groups required for administration will be given full access to the groups. There will be a NUIT infrastructure administration group, this will be restricted to a subset of the NUIT

infrastructure team. These administrators have gone through appropriate IG training. Other groups will be the research admins and users who require access.

During Transit

Replication

DellEMC SyncIQ is used for replication between the two data centres, this is used to replicate data at the share level as a snapshot of the Research Filestore is taken. Any changes made to file or folder are replicated within 60 minutes to the replication point. Synchronisation is facilitated via a dedicated Dark Fibre Connection between the Datacentres using Dedicated Network Interfaces.

User access

During user access the SMB protocol will be used. SMB3.1.1 provide encryption during transit. This utilises AES-128-GCM for encryption, and uses AES256 for all authentication between nodes. For endpoints that can't use SMB3 the following mitigations are in place

- Common desktop – conforming to our policies
- Only allow desktops in specific groups allowed access to the share
- Switched routed network
- Only non-wireless desktops allowed access to the share.
- SMB1 Is no longer enabled
- Linux devices can only access shares via Kerberized NFSv4 ensuring correct user authentication.

At Rest

Physical servers and storage hosting the research filestore are housed in secure, access-controlled datacentres.

When a disk fails, or the disk storage system is decommissioned then the disks are shredded as per Newcastle university policy.

Backup

The Isilon concept allows for high levels of failure safety and Data Security. For data loss to occur Isilon has to fail more than 1 complete node, or more than 3 disks simultaneously on each of the clusters.

When a disk fails, or the disk storage system is decommissioned then the disks are shredded as per Newcastle university policy.

Auditing

Auditing of the security groups are carried as per the FMS Information Governance Steering Group Confidentiality Audit Policy document. This requires that spot checks on what the current membership of the security group is and making sure this checks out with the use who should be in the group.

Firewalls

The network is protected by Fortinet Fortigate 6300 firewalls on the perimeter. The storage servers provide a software based firewall. Both firewalls meet the common criteria. The client systems also

run a firewall. The common criteria and an international standard for computer security certification. For more information please see: http://www.commoncriteriaportal.org/
The firewall will restrict which computers will have access to the server. In addition to the normal servers required for administration by NUIT, each of the servers firewall will use a security group containing the client computers to allow client access to the server.

Secure File Transfer
Secure file transfer is covered under the data sharing policy.

Newcastle University provides a file drop off service that can be utilised to transfer encrypted files. https://dropoff.ncl.ac.uk

For more information regarding the service please see: http://www.ncl.ac.uk/itservice/file-drop-off/

User access

User will access the storage using UNC dfs path, e.g. \\campus\rdw\dsptprojectname. There will be security groups around this to only allow specified and approved toolkit project users access to the share. All users must have passed the IG Training.

Network Security

The campus network is firewalled at the network perimeter. Additional firewalling (using the built-in firewall) is active on servers. All other intermediary network devices are hardened in accordance with vendor recommendations. Network security scanning is continuously performed to identify misconfigured and unauthorised devices. Traffic flows are monitored for network activity (egress and ingress) that may be attributed to malicious software and other forms of malicious activity. Traffic flows that are believed to be malicious are terminated. The private network is segregated from the public network using Network Address Translation and Access Control Lists for traffic management and filtering. The private network is further segregated into wired and wireless security domains, each using different private IP address ranges. All private IP addresses in use across the University consist of IP addresses as defined through RFC1918. Further segregation of network traffic is achieved through the use of VLANs and subnetting.