N/LAB Locally managed IT Systems & Data Policy: Information Security UoN Policy Extension & Implementation Notes

Current version:
VERSION 2.0: 19/09/2023

1. Introduction

N/LAB takes the protection of its locally managed IT systems and data very seriously. N/LAB's locally managed IT systems and data are managed within, conform to, and subject to, the greater University of Nottingham Information Security Policy. This policy and sub-policies are revised as per the revision schedule denoted in the general University of Nottingham Information Security Policy and its sub-policies at a minimum, with sub-policies detailed throughout this document.

In this context "locally managed IT system" refers to **N/LAB servers** owned by the University of Nottingham and hosted by the Nottingham University Digital Technology Services (DTS) Team within a UK based University of Nottingham Data Centre. DTS ensures physical security, network security, backups and hardware monitoring and maintenance in-line with all relevant University of Nottingham Policies. N/LAB locally manage the software on these machines, adhering to and extending the University of Nottingham Information Security and other relevant policies as detailed below. Please read these sections in conjunction with the relevant University of Nottingham Policies (for UoN staff security policies are available here and Research Data Management Policy are available here, these available on request by non-UoN staff). Unless otherwise stated, standards in these policies are directly followed.

2. Relevant terminology

Terminology used in this document is consistent with those in the broader University of Nottingham Policy documents. Relevant definitions for this extension and implementation note include:

- **Restricted data**: Personal: Data that includes personal identifiers and therefore falls under the General Data Protection Regulations (GDPR).
- **Restricted data**: IP and Commercially-Sensitive: Data which has a high commercial value or requires security due to contractual requirements.
- **Confidential data**: Data which has a limited circulation within the University due to commercial or competitive sensitivity.
- **Standard data**: Any data that is freely accessible to all UoN staff and students.
- **Public data**: Any data item that is freely accessible to all parties, whether internal or external.

- **Data Asset Owners:** A Data Asset Owner is the person who is responsible and accountable for:
    - The security of the data asset and access to it.
    - Ensuring the data asset is accurately recorded on the data asset register
    - Nominating data stewards and assigning to them specific responsibilities, authorities or accountabilities for a particular data asset, or an aspect of it.
    - Identifying any additional security controls required to protect the information and working with the system owner to ensure they are implemented
    - Providing guidance to data users on how data sets should be used and protected
    - Ensuring that any licensing or contractual terms that exist for the data asset are understood and adhered to.
    - Ensuring compliance with relevant policies
- **Data Stewards:** A Data Steward's role depends on what the data will be used for. A data asset which will be accessed by only a few people, might not require both an owner and a steward, whereas a data asset which is accessed by several people might require an owner and more than one data steward.

3. Local Policy Implementations / Extensions

A. Data management Plan (including Handling Restricted Data, Legal Basis for Processing, Ethics and Privacy)

Data storage within all N/LAB locally managed IT systems conforms to the University of Nottingham Research Data Management Policy and on a per data asset basis are subject to the University of Nottingham Handling Restricted Data Policy (for UoN staff, available on request otherwise). Implementation details and further restrictions are detailed below:

- The data asset owner for all N/LAB data assets is the N/LAB Data Manager (currently Dr. Gavin Smith).
- The data asset owner is responsible for tasks including:
    - managing access control and data retention inline with any Data Sharing agreements, NDAs and any legal requirements from the data providers and/or research funders
    - user guidance provision
    - data inventory
    - assessing and documenting the **legal basis for processing** when required. **In the case of personal data governed by GDPR** this includes ensuring:
        - When processing personal data, data is processed fully inline with GDPR regulation and according to one of the following legal basis, depending on if the data has been collected directly by N/LAB or if it was provided by a third party
            - the **processing** is necessary for the performance of a task carried out in the public interest
            - the **data subject** has approved consent

            - the **processing** is necessary for the purposes of the legitimate interests of the **data controller** or a third party and the interests of the data subject are not overridden

        - When processing personal data, where appropriate, data may be processed under a **Research and Statistics exemption.** In such cases a review will be undertaken to ensure the relevant conditions apply, including:

            - that complying with the full GDPR provisions would prevent or seriously impair the achievement of the purposes for processing
            - the processing is subject to appropriate safeguards for individuals' rights and freedoms
            - the processing is not likely to cause substantial damage or substantial distress to an individual
            - the processing is not used for measures or decisions about particular individuals, except for approved medical research
            - the research results are not made available in a way that identifies individuals (in the context of right of access)

    - Ensuring data is only granted access for research that is conducted **ethically and with integrity** as governed by the University of Nottingham Ethics and Integrity Policies and overseen by the respective named individuals within these policies. For projects where ethics approval is deemed required, this will be obtained via the appropriate University of Nottingham Ethics committee. Responsibility for ethics approval, if required, will be delegated to an appropriate Data Steward for the Data Asset by the (University of Nottingham) Data Owner.
    - Delegating the responsibility to Data Steward to create **privacy notices** when required according to University Policy and guidance.

- Restricted Data is only stored centrally and securely on the dedicated N/LAB data server (see System Configuration And Management Policy).
- Data from different sources / data sources are securely segregated to meet any data provider / funder / legal requirements
- Restricted Data is accessible only via dedicated whitelisted machines by authorised individuals managed by the University of Nottingham under the relevant Information Security Policies. Data may be processed on these machines, but not stored.
- Restricted Data access is only possible within the University of Nottingham network
- Restricted Data access is subject to all relevant access, logging, monitoring and other policies as detailed in the University of Nottingham Information Security Policy and N/LAB Policy Extension and Implementation Notes
- Confidential Data held by N/LAB is treated identically to Restricted Data
- Standard and Public Data may be additionally stored on University of Nottingham managed IT equipment
- Long term cold data storage, when applicable and subject to and/or to meet any data provider, legal and funder agreements / requirements / timeframes, may additionally be within encrypted containers held on a local N/LAB Backup server and backed up to the University of Nottingham backup system.

B. System Configuration and Management Policy

All N/LAB locally managed IT systems conform to the University of Nottingham System Configuration and Management Policy. Additionally:

- Data is encrypted at rest and during transit
- Data is encrypted before transmission to (1) a local backup server managed by N/LAB and then (2) the University of Nottingham Backup system
- The N/LAB Data Server only permits access to whitelisted Data Access Machines.
- All Data Access Machines must be configured to be encrypted at rest and are regularly checked for compliance by N/LAB staff, in addition to checks under University of Nottingham Policy.
- Data transfers are logged and monitored between the N/LAB Data Server and Data Access Machines to confirm with the above Data Management Policies with respect to Restricted Data.
- Firewalls are correctly configured to enable the above policies and meet security requirements in all policy documents (such as the University of Nottingham IT Network Security Policy)
- All systems will run anti-malware software in accordance with the University of Nottingham Anti-Malware Policy.

C. Access Control Policy

All N/LAB locally managed IT systems will utilise the digital identity management and authentication system provided by the University of Nottingham and governed by its respective policies as detailed in the University of Nottingham Access Control Policy. Access to the University Network and information security training is provided centrally by the University of Nottingham. Access to the specific N/LAB locally managed systems will be granted, documented and revoked by the Data Asset Owner for each asset under principles of least privilege. Access to any locally managed IT systems will be granted, documented and revoked by the N/LAB Data Manager under principles of least privilege. These systems will only be able to be accessed within the University of Nottingham network and will comply with all standards within the University of Nottingham Access Control Policy (including the use of two-factor authentication and access control monitoring and reporting).

D. Logging and Monitoring Policy

All N/LAB locally managed IT systems conform to the University of Nottingham Logging and Monitoring Policy. Additionally:

- Access logging and monitoring of access to the N/LAB Data Server and data transfers from the N/LAB Data Server generates both logs (to a separate, backed up, Graylog server) and alerts to the N/LAB Data Manager which is reviewed and/or actioned in real-time as required. Data transfer alerts are triggered based on command logging and monitoring and data transfer size.

4. Responsible officer

The responsibility for overseeing the implementation and maintenance of these local policy implementation and extensions, as per the University of Nottingham policy, resides with a named individual.

Currently this is: **Dr. Gavin Smith** (gavin.smith@nottingham.ac.uk) [N/LAB Data Manager, UoN]