System Level Security Policy (SLSP)

National Data Integration Tenant

NDIT

National Data Integration Tenant

Contents

Introduction

A system-level security policy is a foundational document outlining the security requirements, responsibilities, and controls for a particular system or set of systems. This policy guides how security should be implemented, managed, and enforced to protect the system's data, users, and infrastructure.

A System Level Security Policy (SLSP) should be documented for all internally or externally hosted system. This is even more important for systems that host personal identifiable information (PII). The template below has been designed to help Information Asset Owner's document the policy.

Acronyms

Examples:

• Personal Identifiable Data	PID
• Personal Identifiable Information	PII
• Data Protection Officer	DPO
• Senior Information Risk Owner	SIRO
• Secure Consulting Team	SCT
• Cyber Security Operations Centre	CSOC
• Network & Information System	NIS
• Transport Layers Security	TLS
• Software as a System	SaaS
• Infrastructure as a Service	IaaS
• Platform as a Service	PaaS
• Role Based Access Control	RBAC
• Discretionary Access Control	DAC
• Mandatory Access Control	MAC
• Attribute Based Access Control	ABAC
• Rule Based Access Control	RBAC
• User Based Access Control	UBAC

Completion Notes

Please ensure that all columns are completed. If you are unsure, please contact the **Security Consultant** who will provide you with assistance.

If a question is not relevant, please mark it as N/A.

Once the SLSP form is completed, please email it to the NHS England Security Consultant. They will review and provide feedback. Please be advised that once you have completed the form there may be further questions.

1.0	**Governance**	
1.1	System Owner (must be a named individual):	Lucy Ellis Brookes
1.2	Information Asset Owner (IAO):	Data Set Owners
1.3	Information Governance (IG)/ Privacy, Transparency, and Trust (PTT):	Jackie Gray
1.4	Senior Information Risk Owner (SIRO):	?
1.5	Security Consultant:	*Sadi Sengel*
1.6	Approved by:	*Peter Barrett*
1.7	Approved date:	*18th July 2025*
1.8	Next review date:	*June 2026*
1.9	Version:	*1*
1.10	System Operational Status	*MVP*
1.11	Completion / Go-live date:	*2025*
2.0	**Description/ Purpose of the System**	
2.1	System Name:	NDIT National Data Integration Tenant
2.2	System Owner (must be a named individual):	Lucy Ellis Brookes
2.3	*Detailed overview and purpose of the system* *What is the system? What does it do?*	**National Data Integration Tenant (NDIT)** will be the secure national safe haven for data collection, processing and management for NHS England, including for the processing of identifiable data.
2.4	*Scope/Access of the system*	Data will be submitted via federation with Local FDP tenants.
2.5	*Doe the system use shared resources:* ***Yes/No*** *If yes what are the shared resources?* e.g shared CPUs/RAM/Storage/network	Yes Will be sharing FDP resources

	interfaces/databases with logical separation/virtual machines/identity services etc	
2.6	*Is the system comprised of multiple systems:* ***Yes/No*** If yes, please list them	No It is a sub system of FDP
2.7	System Category	*Critical*
2.8	System users	*FDP Tenants, and Non FDP Providers*
2.9	What is the Data Classification of the system? What is the data risk profile class according to the Health & Social Care Data Risk Model	*Class 5*
3.0	**System Architecture**	
3.1	Provide a high-level architecture of the system.	Yes
4.0	**Coud Architecture**	
4.1	Is a cloud solution being used? **Yes/No**	Yes
4.2	If yes, what deployment method • Public • Private • Hybrid	Private
4.	If yes, what Service Model (delete as appropriate): • SaaS • PaaS • IaaS	SaaS
4.	Is the cloud provider NIS compliant? **Yes/No**	Yes

4.	Is the cloud provider GDPR compliant? **Yes/No**	Yes
4.	Where is the data hosted and processed?	UK
4.	Where are the backups stored?	UK
4.	Is there a Service Level Agreement in place? **Yes/No** If yes, where is it located?	Yes
5.0	**Software**	
5.1	Details of software stack where applicable – What software is being used within the system environments and for development? E.g. programming language, platforms being used	FDP tools - Palantir Foundry
6.0	**Hardware**	
6.1	Details of hardware – What hardware is being used?	NA
6.2	Is there an external client-side component other than a basic browser? **Yes/No**	No
6.3	Does the system use a client PC to hold information e.g. cookies? If yes what information is retained and under what retention?	No
7.0	**Data Encryption**	

7.1	Details of the data collected and recorded on the system e.g. PID/PII	PID and Non PID
7.2	If there is PID or PCD data held on the system what measures are in place to ensure content is not cached on external PCs?	Only accessible by a web browser, content is not cached
	How is the data transfer between the system and the external client PCs secured?	No data transfer allowed.
7.3	How is data encrypted **In Transit**?	NDIT uses robust, modern cryptography standards. https://app.safebase.io/accounts/c9c9a7b1-6d2a-4b12-b64f-def65ae67649/share?product=default&itemUid=4ea65d1e-79fb-47cf-95a8-bdb24d2d6a4b&source=title
7.4	How is data encrypted **At Rest**?	NDIT uses robust, modern cryptography standards. https://app.safebase.io/accounts/c9c9a7b1-6d2a-4b12-b64f-def65ae67649/share?product=default&itemUid=ef061e5b-a2f4-469e-92bc-ab973e3d7842&source=search
7.5	How is data encrypted **In Use**?	Palantir Encryption mechanism is used when in NDIT. PET used when transferring to FDP.
7.6	Where are encryption keys stored and what measures are in place to ensure key management security?	The backing Key Encryption Keys (KEKs) for object store data are generated and stored inside key management systems managed by Palantir such as AWS Key Management Service, Microsoft Azure Key Vault, or GCP Key Management Service.
7.7	How are encryption keys rotated and managed?	Palantir Security White Paper. Needs NDA
7.8	Who is responsible for managing and	SaaS provider

	enforcing encryption policies?	
7.9	Is sensitive data automatically encrypted in all locations, including databases, files backups?	Yes
7.10	How is encryption applied to data in the cloud and are cloud provider encryption practices reviewed?	Managed by Palantir
7.11	Is there a process for auditing encryption effectiveness and updating standards? Please provide details.	Managed by Palantir
7.12	Are decryption capabilities restricted to only those who need and is MFA enforced for decryption actions?	Yes, Yes
8.0	**Data Quality**	
8.1	Details of any data quality requirements	Data Quality team exist
9.0	**Data Retention**	
9.1	What are the data retention periods for different categories of data, and do they comply with regulatory requirements?	Retention periods are set by NHSE Policies for various categories. NDIT is complaint with those.
9.2	Who is responsible for managing and reviewing data retention schedules to ensure compliance?	Data Set owners decide under the guidance of FDP Data Governance Group.
9.3	Are there automated processes to manage the retention and deletion of data when	YES

	retention periods expire?	
9.4	How are exceptions to data retention policies documented, approved, and tracked?	Data Set owners decide under the guidance of FDP Data Governance Group.
10.0	**Data Backups**	
10.1	Details of any data backup arrangements	SaaS provider manages this on instruction from NHSE
10.2	What is the backup frequency for data?	1 Hour
10.3	Where are backups stored and are they securely protected against unauthorised access?	Immutable, SaaS provider manages this on instruction from NHSE
10.4	Are backups encrypted both at rest and in transit? Please provide details of how they are encrypted both at rest and in transit.	Yes, modern using robust, modern cryptography standards.
10.5	Is there a process to test the restoration of backups to verify data integrity and recovery speed?	SaaS provider manages this
10.6	How long are backups retained and does this comply with regulatory and organisational (NHS E) data retention policies?	Yes, 14 days
10.7	What access controls are in place to restrict who can create, modify and delete backups?	Immutable, inaccessible to users, SaaS provider manages this
10.8	Are backups configured to be immutable? (Preventing	Yes

	unauthorized or accidental alterations/deletion)	
10.9	How long is data in immutable backups stored and does this comply with regulatory and organisational requirements?	Yes, 14 days
10.10	What processes are in place to monitor and enforce immutability of backups?	See added Document
10.11	Are immutable backups stored in an isolated environment?	Yes
10.12	Is there versioning enabled for immutable backups to enable recovery from various points in time?	Yes
10.13	How frequently are immutable backup configurations reviewed?	Annually
11.0	**Data Sanitisation, Destruction, Disposal/Deletion**	
11.1	Details of data destruction/disposal/ deletion process.	All Palantir software products and infrastructure are designed to comply with the strictest data deletion and erasure requirements. For further information on deletion, please see our published blog post: https://blog.palantir.com/designing-for-deletion-palantir-explained-6-adfe25fda810
11.2	What methods (e.g. degaussing, cryptographic erasure) are used to sanitise data from storage media?	See above
11.3	Are data sanitisation procedures documented and aligned with industry	See above

	standards (NIST 800-88)	
11.4	Is there a process to verify and certify that data has been completely sanitized after deletion?	See above
11.5	Are employees trained on secure data sanitisation practices, for portable media and end of life devices?	See above
11.6	What controls are in place to ensure third-party providers follow sanitisation requirements when handling NHS E data?	See above
11.7	What procedures are in place to securely dispose of data, including physical media and digital records?	See above
11.8	Is data disposal verified and logged to ensure compliance with data protection policies?	See above
11.9	Are third-party vendors required to follow secure data disposal practices, and is compliance verified?	See above
11.10	How are devices containing sensitive data (e.g., hard drives, USBs) securely disposed of or destroyed?	See above
11.11	Is there a process to ensure that data is completely removed	See above

	from cloud environments when disposal is required?	
11.12	Are employees trained on secure data disposal practices, especially for mobile devices and end-of-life equipment?	All Palantir employees undergo rigorous, multi-faceted information security training at least annually.
11.13	How frequently are data disposal methods and policies reviewed to ensure alignment with regulatory standards and best practices?	Annually
12.0	**Secure Coding**	
12.1	Is there a code review process to identify and address security flaws before deployment?	Yes
12.2	Are automated tools used to scan for vulnerabilities in code during development? If so, what tool are being used?	Yes
12.3	How is sensitive data protected within code to prevent exposure? E.g. PII, credentials	Markings and security controls, all SaaS
12.4	Is there a process to address security patches and updates in third-party libraries	Yes
13.0	**Load Testing**	
13.1	Is loading testing conducted to assess system performance under peak conditions?	Yes
13.2	How often is load testing conducted?	Functions • Unit testing • Getting started • Palantir
13.3	What metrics are tracked during load	Functions • Unit testing • Getting started • Palantir

	testing to identify potential performance bottlenecks?	
13.4	Are security implications considered during load testing to ensure system availability and integrity under stress?	Yes
13.5	Is there a process for stimulating different types of traffic patterns to ensure system resilience?	Yes
14.0	**Access Control Models**	
14.1	What access control model(s) e.g. RBAC, ABAC, MAC, DAC are implemented and are they relevant to the organisation's requirements?	https://nhs.sharepoint.com/:w:/r/sites/FederatedDataPlatformSupplierCollaborationsite/_layouts/15/doc2.aspx?sourcedoc=%7BEC2C8A5D-8F0E-4C7E-AFD2-5C8AF317A326%7D&file=FDP%20NIDCI%20User%20Access%20Model.docx&action=default&mobileredirect=true&DefaultItemOpen=1
14.2	How are user roles and permissions defined? Are they aligned with the principle of least privilege or any other …?	Data Set owners decide. NDIT users authenticate using a IDAM provider with 2FA. The IDAM provider can vary dependant on the single sign-on policy of the tenant owner. Access to NDIT data and applications (authorisation) is controlled via the Foundry platform. FDP utilises a purpose-based access control system. Access to data and applications is restricted by RBAC controls and further limited to specific purposes for access.
14.3	What is the timeout period for inactive accounts?	3 Months
14.4	What is the timeout period for inactive sessions?	3 Months. Data Set owners review access lists on a biannual basis. Any inactive accounts are removed after 3 months of

	Who/What monitors session activity?	inactivity. Access to the platform is integrated to the starters, leavers and movers process within the local organisation
14.5	What are the login and requirements? What is the password length requirement and what are the password complexity rules? Is there 2fa?	The password complexity is set by the IDAM solution. In the case of the National tenant, this is >8 characters including mixed case and special characters. 2FA is also mandatory for all FDP users.
14.6	How is access to privileged accounts managed, is multi factor authentication enforced?	MFA, yes
14.7	Is MFA implemented for all users? What MFA method(s) is used and are there any exceptions to when MFA is applied?	Yes
14.8	If the system requires a separate login, what password length/complexity rules are applied?	NA
14.9	How will the system deal with failed logon attempts?	Via the specific process connected with the selected IDAM provider.
14.10	How will access attempts be monitored and audited to confirm that these controls are working?	Via the specific process connected with the selected IDAM provider
14.11	What is the maximum permitted time that a session can remain active before the user	24 Hours

	is required to reauthenticate?	
14.12	Is SSO supported? If yes, is it enabled?	Yes, yes
14.13	How will an Information Asset Owner (IAO) monitor and audit to confirm that these access controls are working?	For authentication, this will be via the specific process connected with the selected IDAM provider. NDIT maintains detailed audit logs of all user actions and system events, which can be used to detect and investigate potential security incidents. This includes logging of cryptographic operations and key usage. FDP is also integrated with NHS CSOC. PET also has internal security monitoring administered by the Iqvia platform team, as well as CSOC integration.
15.0	**Access Configuration and Rights**	
15.1	Who is responsible for controlling access to the system?	Data Engineering, NHSE
15.2	Is there an administrator role for the system?	Yes
15.3	How many administrator roles are there?	1
15.4	How is the administrator role configured/setup?	As per NHSE Policies
15.5	Does administrator have two separate accounts? (One to perform administrative duties and one to perform non-admin duties)	Yes
15.6	How are Enterprise Admin roles controlled?	As per NHSE Policies
15.7	How do internal users log in to the system?	2FA with nhsmail

	Eg. Username/password/ID/Pin	
15.8	How is the internal access configured/setup?	A combination of RBAC and Purpose Based access controls
15.9	Is internal access unrestricted? **Yes/No** If yes, please explain how.	No
15.10	How will internal access be managed/monitored?	NHS CSOC Monitoring
15.11	How is external access initially set up?	External Access is disabled by default
15.12	How do external users log on to the system?	All access is 2FA via either NHS Mail (NHS staff) or Okta (External Users)
15.13	Is External access unrestricted? Yes/No If yes, please explain how	No
15.14	Will any external users have administrative access?	No
15.15	How will external access be managed/monitored?	NHS CSOC Monitoring
15.16	Who monitors account inactivity? Is there an automated system to monitor user activity?	FDP Service Management Team
16.0	**Access Control Policies/ Processes**	
16.1	Do you have an Access Control Policy? If yes, please provide a copy.	https://app.safebase.io/accounts/c9c9a7b1-6d2a-4b12-b64f-def65ae67649/share?product=default&itemUid=ddee6fb4-ffcc-40bc-892c-ca344768d1ff&source=search
16.2	What is the process of configuring Access control models that are being implemented?	The access control policy is the default setup
16.3	How is Access Control managed? What is the	FDP Onboarding and Offboarding (SOP) See added document

	user onboarding and offboarding process/procedure for internal and external users?	
16.4	What is the process for dealing with failed login attempts?	Via the specific process connected with the selected IDAM provider.
16.5	What is the process when a user no longer requires administrator access?	FDP Policies, user is removed or privileged access is revoked
16.6	What is the process when users forget their log in details?	FDP Policies / NHS Mail Policies NHSmail 2 Portal - Home
17.0	**Security/Pen Testing – Please note you may be required to provide a copy of the latest Pen Test Report**	
17.1	When was the last Pen Test conducted?	In planning stage, new system, first SLSP
17.2	When is the next Pen Test scheduled?	Autumn 2025
17.3	What is the Frequency of Pen Testing and are they conducted for both internal and external systems?	Annual
17.4	Are third party suppliers used for Pen Testing? Are they certified and vetted for compliance?	Yes
17.5	How are Pen Test results documented?	Reports are sent to select NHSE staff and tracked in Confluence/Jira
17.6	Where are the reports stored/saved?	Confluence
17.7	Has an action/remediation plan from the last test been compiled? (Please provide a copy)	In planning process
17.8	Who is responsible for tracking the remediation plan?	Director of Platform Security

17.9	Where is the action/remediation plan kept?	Programme Confluence pages
17.10	What measures are taken to ensure findings from previous Pen Tests are verified for effective remediation?	Fixes are pushed and tested to ensure that the vulnerabilities are address. In the case of significant vulnerabilities a retest may be used to further validate.
17.11	Is re-testing conducted to confirm that vulnerabilities have been successfully addressed?	In most cases
18.0	**Vulnerability and Patch Management**	
18.1	Do you have a vulnerability and Patch Management Policy in place?	Yes
18.2	Please provide details of the vulnerability management plan.	NHSE Policies, managed by Cyber Operations NHSE, CISO function.
18.3 Roles & Responsibilities	Who is responsible for vulnerability management?	Palantir are responsible for the underlying Foundry Platform NDIT is integrated with CSOC for monitoring, NHSE Cyber Ops oversee and validate
18.4	What are the specific roles of IT, Security teams and third-party vendors in vulnerability identification and remediation?	Palantir Security team checks and controls the underlying infrastructure. NHSE Cyber Ops monitor, oversee and validate
18.5	How is accountability ensured for remediation tasks and who signs off resolution?	SIRO
18.6 Identification& vulnerability management	How are vulnerabilities identified within a system?	Palantir are responsible for the underlying Foundry Platform CSOC monitoring Annual Pen Testing at a minimum Potential for future Red Team engagement

18.7	What tools and processes are used for continuous vulnerability scanning and monitoring?	CSOC monitoring and SaaS Provider hosted tools.
	How often are vulnerability assessments performed? (e.g. daily, weekly, monthly)	Continuous monitoring
	What sources are used to stay up to date on emerging vulnerabilities? (e.g. CVE databases, vendor notifications)	Palantir Security team, OWASP, NHS CSOC
18.8	What actions are taken if a vulnerability is exploited?	Palantir internal security team works with NHSE CSOC
18.9	How does vulnerability management process integrate with the incident management plan?	NHSE Policies (Vulnerability and Patch Management Controls Standard. Palantir maintains a thorough Vulnerability Management and Patching program. Vulnerabilities and findings are prioritized based on criticality, severity, and impact and tracked through an internal ticketing system. Patches and configuration changes are pushed out using Palantir's Change Management procedures based on internally published patching SLAs. Read more about Palantir's patch management process in our blog post on continuous vulnerability scanning at scale.
19.0	**Risk Assessment**	
19.1	Details of risk assessment and next review date	*Hasn't completed yet. (Risk assessment of the proposed system needs to be done prior to commencement of work as a minimum it should have a risk to confidentiality, integrity and availability of the data it will process)*
19.2	Does the system comply with the organisations risk appetite?	Yes
19.3	How are identified vulnerabilities	NHSE Policies (Vulnerability and Patch Management Controls Standard. Palantir

	prioritised based on criticality?	maintains a thorough Vulnerability Management and Patching program.
19.4	What criteria is used to assess the risk level of a vulnerability? (e.g. CVSS, potential impact)	NHSE Policies (Vulnerability and Patch Management Controls Standard. Palantir maintains a thorough Vulnerability Management and Patching program.
19.5	What is the threshold for classifying a vulnerability as critical, high, medium or low risk?	Palantir's patch management process in our blog post on continuous vulnerability scanning at scale.
19.6	Who is responsible for determining the severity of vulnerabilities and their impact on business operations?	FDP Platform support, FDP Service Management
20.0	**Protective Monitoring**	
20.1	Is there protective monitoring on this system? E.g. Firewall, Intrusion Detection, Intrusion Prevention Please provide details of what tools are being used and what is being monitored.	*Yes, FDP provides*
20.2	Is there continuous security monitoring implemented? Please provide details	*Palantir and NHSE CSOC teams*
20.3	What logs are collected?	NHS CSOC decides during the onboarding process.
20.4	Where are the logs analysed?	NHS CSOC environment keeps copies of the logs
20.5	Who is responsible for protective monitoring?	Palantir Security Team,
20.6	Has the program/system been onboarded with CSOC? If yes, please	Yes

	provide the onboarding document. If no, the program/system will need to be onboarded. (Security Consultant will provide you with these details)	
20.7	When was the onboarding document last reviewed?	Not Yet
20.8	Have you had a service review meeting with the SoC in the last 12 months?	Not yet
20.9	Have you reviewed you protective monitoring use cases in the last 12 months	Not yet
20.10	What is part of the system is CSOC monitoring?	TBC
21.0	**Security Incident Management and Reporting**	
21.1	What is the security incident management procedure? How are the IT/IG/Cyber teams informed and involved?	*NHSE and FDP Incident management procedures. NHSE Service Management processes apply*
21.2	Who is responsible for incident management?	NHS CSOC and Palantir CSOC teams works together
21.3	What are the specific roles of IT, Security teams and third-party vendors in incident identification, management and remediation?	NHS CSOC supporting Palantir

21.4	How is accountability ensured for remediation tasks and who signs off resolution?	SIRO
22.0	**Business Continuity**	
22.1	Provide details of your business continuity plans.	Palantir maintains this policy internally. This policy is audited internally by our ISMS committee, and externally by auditors as part of our various compliance and regulatory accreditations. https://app.safebase.io/accounts/c9c9a7b1-6d2a-4b12-b64f-def65ae67649/share?product=default&itemUid=f8a6e2f1-82d6-4ec9-9836-4b737f74a89a&source=search
22.2	How frequently are business continuity plans and associated systems tested and are tests reviewed for effectiveness?	See above link
22.3	Are backup and failover systems in place and accessible to support continuity if primary systems become unavailable?	See above link
22.4	Third Party Supplier Contract Clauses	There is a contract between NHSE and Palantir
22.5	Intellectual Rights	Stated in a Contract between NHSE and Palantir
22.6	End of Contract Data Deletion/Return	Stated in a Contract between NHSE and Palantir
22.7	Subject access requests/ functionality to respect objections/withdrawal of consent	Stated in a Contract between NHSE and Palantir
22.8	Any specific requirements regarding consent and disclosures of information	Stated in a Contract between NHSE and Palantir
23.0	**Relevant Legislation / Contractual Obligations**	
23.1	Is the system classed as an essential service	No

	under NIS legislation? **Yes/No**	
23.2	Details of any specific legislation e.g. Mental Capacity Act 2005, Children Act 2004	N/A
24.0	**Audit**	
24.1	Provide a description of auditing capabilities of the application and supporting infrastructure	For authentication, this will be via the specific process connected with the selected IDAM provider. FDP maintains detailed audit logs of all user actions and system events, which can be used to detect and investigate potential security incidents. This includes logging of cryptographic operations and key usage. FDP is also integrated with NHS CSOC. PET also has internal security monitoring administered by the Iqvia platform team, as well as CSOC integration.
24.2	Details of who is responsible for auditing compliance. e.g. confidentiality audits. (Name and Role)	IAO