

CODE OF CONNECTION

For

NORTHERN IRELAND CIVIL SERVICE NETWORKS

Version 1.0

18 May 2009

DF1/08/201217

NICS CODE OF CONNECTION
(Not Protectively Marked)

NICS CODE OF CONNECTION
(Not Protectively Marked)

CONTENTS		Page
1	NICS Departmental Code of Connection	5
2	Code of Connection for Third Parties	9
3	Code of Connection for End Users	29
Appendix 1	Compliance Statement for Connection to Network NI	30

NICS CODE OF CONNECTION
(Not Protectively Marked)

NICS Code of Connection	Version 1.0
DID Reference	DF1/07/16889
DATE	May 2009
AUTHOR	Colin Lobo, Deloitte Network NI team
OWNER	NICS Accreditation Panel

Version Control

Version 0.1	Draft for comment by NICS Accreditation Panel, ITSO Forum and IA Policy Working Group
Version 0.2	Updated draft
Version 1.0	Approved for issue

NICS CODE OF CONNECTION
(Not Protectively Marked)

SECTION 1

NICS Departmental Code of Connection

This section describes the requirements that all departments must comply with when implementing line of business applications regardless of whether IT Assist will be providing support for the application or the server it will reside on. 'Line of business' refers to the activity for providing the services of a particular department.

This code of connection will also apply to any Non Departmental Public Body (NDPB) or agency who wishes to connect to the NICS. If the NDPB/agency network is not accredited to a level commensurate with a protectively marked RESTRICTED network, then they will need to comply with the requirements defined in Section 2.

Any line of business application or service that is not provided by IT Assist must have its own Risk Management Accreditation Document Set (RMADS). As a minimum, the points detailed below need to be included within the RMADS.

Ref	Requirement
NICS.1	<i>Security Responsibilities</i> The department must have clearly defined security roles and responsibilities.
NICS.2	<i>User Policies</i> If the existing policies do not encompass the usage requirements for the application/system, then an addendum should be created for the existing policy/policies or a specific one should be created.
NICS.3	<i>Users Awareness</i> If new technologies are being introduced that could pose a new risk to the IT environment or the data within it, then appropriate user awareness training must be conducted.
NICS.4	<i>Roles</i> Where necessary, appropriate measures must be in place to ensure that adequate role segregation is in place.
NICS.5	<i>Legislation</i> The system/application must comply with all relevant legislation and adhere to the security policies that are applicable to the services provided by the IT Assist.
NICS.6	<i>Network Connectivity</i> If the system/application will require new network connectivity to external parties or an extension to existing external connectivity, this must be discussed with the IAT. Additionally, the provider will need to complete a Code of Connection document.

NICS CODE OF CONNECTION
(Not Protectively Marked)

Ref	Requirement
NICS.7	<p><i>Wireless Networking</i></p> <p>The IAT must be involved in the implementation of any new wireless installations. Where the wireless network will have a connection to the NICS network, the ownership of such installations will rest with the IT Assist as this will form part of the core network infrastructure.</p>
NICS.8	<p><i>Third Party Connectivity</i></p> <p>In the event that a third party requires either temporary or permanent access to a system or application that they support, this must be referred to the Accreditation Authority before access is granted.</p>
NICS.9	<p><i>Use of Encryption</i></p> <p>Should the department have a requirement to implement encryption technologies, the IAT must be involved to ensure that all the supporting process (i.e. key management, key revocation etc.) are properly addressed.</p>
NICS.10	<p><i>Protective Marking</i></p> <p>The Accreditor must be consulted before any protectively marked data is exchanged with a system that has a lower protective marking than the host system (i.e. from Impact Level 3 (IL3) to IL2 or IL1).</p> <p>If there is a requirement to connect a system or store data that has a protective marking higher than Impact Level 3 (RESTRICTED), the Accreditor must be consulted first to ensure that appropriate measures are in place to secure the data/system.</p>
NICS.11	<p><i>Access Control</i></p> <p>If the department has a specific requirement for enhanced access control measures to be in place, they must discuss this requirement with the Departmental IT Security Officer. Examples could include restricting access to financial or personal data.</p> <p>For any line of business application that the department wishes to implement, appropriate access control measures must be available.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Ref	Requirement
NICS.12	<p><i>Audit Trail</i></p> <p>Any system or application that is implemented must be capable of providing an audit trail in line with HMG Memo 22. In summary, this must include the following information:</p> <ul style="list-style-type: none"> • Session start and end time; • Unique user account that was used to logon; • Any administrative activity that was performed; • Failed attempts to logon or access an object; • Where the audit trail information will be stored and the length of time that it can be stored for; and • The mechanisms available to interrogate the audit log. <p>The departmental IT Security Officer should be consulted to ensure that appropriate auditing is in place, adequate provision is made for storing the logging data and that the logging information can be easily interrogated.</p>
NICS.13	<p><i>Security Monitoring</i></p> <p>The department must provide details as to how they will fulfil their security monitoring obligations if this will not be undertaken by the IT Assist.</p>
NICS.14	<p><i>Data Storage Requirements</i></p> <p>Where IT Assist will be backing up the data for the department and there is a requirement for special considerations to be factored in, the departmental IT Security Officer must be consulted. The assumption should be made that all NICS data will be backed up to shared media and will not be backed up in isolation.</p>
NICS.15	<p><i>Patching and Anti Virus</i></p> <p>Where the department is managing the server/s that will be connected to the NICS core network and have the responsibility for patching and AV updates, details must be provided to the IT Assist Security Manager as to how this will be achieved.</p> <p>Only in exceptional circumstances should the IT Assist patching and AV controls not be used in preference to alternative arrangements.</p>
NICS.16	<p><i>Asset Register</i></p> <p>The department must maintain an asset register for systems that they are responsible for.</p>
NICS.17	<p><i>Incident Management</i></p> <p>Where the main NICS incident handling, management and escalation procedures will not be used, the department must make arrangements to ensure that all affected staff knows what the revised processes are.</p> <p>To support this, an incident log should be maintained and reviewed on a monthly basis.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Ref	Requirement
NICS.18	<p data-bbox="357 277 539 304"><i>Change Control</i></p> <p data-bbox="357 313 1155 427">Where a system is connected onto the NICS core network which is maintained by the department, the IT Assist Security Manager must be informed of any security related changes before they are made to the system. This should be accompanied by an impact assessment.</p>
NICS.19	<p data-bbox="357 441 552 468"><i>Physical Security</i></p> <p data-bbox="357 477 1155 591">Where servers are to be hosted in departmental premises, appropriate measures must be taken to ensure that access to the server room is controlled. Measures must be taken to prevent unauthorised users from gaining access.</p> <p data-bbox="357 600 1155 680">Under no circumstances should the department connect equipment to the NICS core network unless this has been approved by the IT Assist Security Manager.</p>

SECTION 2

Code of Connection for Third Parties

This code of connection (CoCo) section provides details of the requirements that must be adhered to by any party who will be providing IT related services to the Northern Ireland Civil Service (NICS) via IT Assist or any other means. All references to **Contractor** relate to a third party and/or a subcontractor who will be providing services to the NICS.

The **Contractor** must complete this Appendix stating for each requirement how they will be achieving compliance or not as the case may be. Responses should be provided for each point detailed either in the tables below or using the reference numbers within the table.

For the remainder of this document, reference will be made to NICS regardless of whether the service provision/connection is direct to the line of business system, via Network NI, or directly to IT Assist.

Purpose

There are a number of requirements (legislative and others issued by the Cabinet Office on behalf of the National Technical Authority for Information Assurance) that the NICS must adhere to. Where third parties are involved in service provision, they must demonstrate to the NICS IT Assist Security Authority and the NICS Accreditation Panel that these requirements have been factored into their service provision. In the majority of instances, the same requirements that are placed on IT Assist will also be applied to the provider and they will need to demonstrate their compliance with this. In many cases, this will take the form of a Risk Management Accreditation Document Set (RMADS) that the IT Assist Security Manager and/ or the NICS Accreditation Panel will be an Accreditor of.

Scope

This code of connection applies to the following:

- Any third party who hosts or provides access to systems/applications, data or provides IT services to the NICS;
- Any third party who provides software applications or services to the NICS; and
- Any third party who provides remote system or application support to NICS.

Depending on the service being provided, some of the points within the CoCo will be irrelevant. However, the **Contractor** must state that this is the case in their compliance statement response/Risk Management Accreditation Document Set.

Regardless of whether there is a direct network connection to the NICS or not, this document will be applicable.

Right of Access/Audit

Authorised NICS personnel (or their Contractors) will have the right to audit and review the configuration of/protection provided by systems and data that are being hosted by

NICS CODE OF CONNECTION
(Not Protectively Marked)

third parties. The purpose of this will be to provide assurance to the NICS Accreditors that the systems have been configured in accordance with the supporting RMADS and is compliant with this CoCo.

The remainder of this section details all the various aspects that the provider will need to demonstrate to the NICS/ IT Assist. Where an RMADS is being produced, compliance and confirmation of provision of these facilities must be included within the document. If a RMADS is not being submitted, then this document must be used to provide details of how the provisions will be met.

Re-Accreditation

Unless the Accreditor has specifically agreed an exception, all systems will be subject to re-accreditation annually.

However, in the event of any of the following, re-accreditation may be required immediately. Reference must be made to the Accreditor:

- A reduction in the minimum security clearance level (i.e. Security Cleared);
- Changes or major upgrades to the IT system (e.g. operating system) within the environment;
- Major changes or upgrades to the application or system management facilities;
- Changes that result in a significant increase in the number of remote users providing support or the use mobile devices for remote management;
- Additional network connections made to other environments;
- If the IT environment hosting the NICS systems or the immediate hosting physical facilities are shared with another party;
- Relocation of the IT system to new premises;
- Asset values change (e.g. protective marking exceeds RESTRICTED);
- The nature of threats or vulnerabilities is perceived to have changed significantly;
- A major security incident; or
- A reduction in the level of physical security controls.

IT Health Checks

Every system will be subjected to an IT Health Check (ITHC) where compliance against this code of connection and any other relevant policy documents – including the RMADS – will be assessed. Generally, an ITHC is conducted annually unless the Accreditor has determined that it should be performed more frequently. In the event of the system/application being subject to re-accreditation, then an ITHC would be required. The **Contractor** will need to provide adequate access and connectivity to allow the ITHC to take place.

NICS CODE OF CONNECTION
(Not Protectively Marked)

Security Governance

The **Contractor** will need to demonstrate to the NICS that appropriate security governance arrangements, measures and organisational support is in place to protect the data, information, systems and services provided to the NICS. Supporting information as to how this will be achieved, the processes that will be put in place and where compliance has not been obtained must be documented within the RMADS.

Security Organisation

Ref	Requirement
SG.1	<i>Security Responsibilities</i> The Contractor must provide details of their security policy, the measures that are in place to implement, maintain and monitor it and those who have a defined role within the organisation in supporting the policy.
SG.2	<i>Security Liaison</i> A dedicated person should be nominated within the Contractor's organisation to assume responsibility for all security matters that are relevant to the services being provided to the NICS. This will include all assets as well as the provisions that the supplier will be making.

Other Supporting Policies

Ref	Requirement
SG.3	<i>Service Specific Policies</i> Details must be provided of specific policies that have been created to support the service offering to the NICS. This must include provision for all legislative requirements that the NICS must adhere to (e.g. Data Protection Act, Freedom of Information, Payment Card Industry Data Security Standard etc.) and any other requirements that have been placed on the supplier by the respective NICS department to mitigate identified risks.

NICS CODE OF CONNECTION
(Not Protectively Marked)

User Awareness

Ref	Requirement
SG.4	<p><i>User Awareness Information</i></p> <p>The requirements placed on Government systems are different and more demanding than many other business communities. The supplier must provide details of how this information is communicated to those who will be involved in the service provision to the NICS and where/how it can be accessed within their organisation.</p> <p>Details should also be included of the frequency with which it is updated and the method that is employed to communicate this to the Contractor's staff and how a record is maintained for those involved with the service provision to note that they have been made aware.</p>

Employment Screening

Ref	Requirement
SG.5	<p><i>Employment Checks</i></p> <p>Details should be provided of the processes that are used to undertake pre-employment checks of those who will be involved in supporting the NICS applications/systems. This should also include the processes that are used for sub-contractors.</p>
SG.6	<p><i>Security Clearances</i></p> <p>Details must be provided of the security clearance levels that have been/are being obtained for staff who will be accessing and supporting the NICS systems and data. Details must also be provided of the clearance level in relation to the functions that the role would undertake (where applicable e.g. system administrator, help desk staff etc.).</p> <p>A process must be in place to monitor these clearances and provisions must be in place to ensure that clearances are renewed prior to their expiration.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Segregation of Duties

Ref	Requirement
SG.7	<p><i>Roles</i></p> <p>It is likely that there will be situations where it is essential that segregation of duties is enforced. An example being different staff should be involved with the administration and monitoring processes. The Contractor shall provide details how this will be implemented (whether procedural or technical) and how the situation will be reviewed.</p>

Compliance with Legislation

Ref	Requirement
SG.8	<p><i>Data Protection Act 1998 (DPA)</i></p> <p>The Contractor shall comply with the DPA and will provide details as to how it will secure the NICS's data.</p>
SG.9	<p><i>Other Applicable Legislation</i></p> <p>The NICS will provide details of any other legislation that will be applicable which could be dependant on the services and systems being provided. Examples of such legislation will be the Freedom of Information Act which could extend to the Contractor, the Official Secrets Act etc.</p>

Network and Communications

The integrity and security of the NICS network perimeter is paramount, both from the perspective of maintaining security of the internal systems and networks, but also from the point of view of meeting the requirements of other external networks with which the NICS will connect to, specifically the GSI. Consequently, all external providers to NICS must ensure that they provide an adequate level of security to protect the NICS systems and networks.

The following requirements relate to third party providers who will be connecting to Network NI network infrastructure and will be providing services to the NICS via IT Assist or directly to a NICS Department.

“*External network segments*” include (but are not limited to):

- Non IT Assist, NICS Departmental, or Network NI managed network segments;
- Third party support links/connections;
- External agencies and Non Departmental Bodies (NDPBs);
- LAN segments/physical network infrastructure in buildings shared by the NICS departments with other organisations (both public/private sector);
- Corporate/shared networks of existing or future outsourcing suppliers;
- Government or other public sector managed networks (including GSI, GSX, xGSI, GSE, etc.);
- The public Internet;
- Any other network not explicitly comprising the Network NI network service.

NICS CODE OF CONNECTION
(Not Protectively Marked)

Connectivity to the NICS and IT Assist

Ref	Requirement
NW.1	<p><i>Connectivity Method</i></p> <p>The Contractor must provide details of the network technology that will be used to connect to the NICS (e.g. MPLS, fixed line, Internet etc.). Details should also be provided of any Accreditation or approval that this technology has been awarded. Details of any supplementary protective controls that have or will be implemented must be provided.</p>
NW.2	<p><i>Firewall protection</i></p> <p>Any connection between IT Assist or any NICS network must be protected by an appropriately configured firewall. The firewall must be configured to provide the maximum level of security possible whilst meeting the business and technical requirements for the connection.</p>
NW.3	<p><i>Shared Connectivity</i></p> <p>Details must be provided where any connectivity components (i.e. firewall, switches etc.) that are used to connect to the NICS are shared with other external (to both NICS and/or the Contractor) parties. Details of the protective controls that have or will be implemented must be provided.</p>
NW.4	<p><i>Onward Connectivity</i></p> <p>Details must be provided of any other network connectivity that will be in place to the Contractor's own corporate systems (i.e. their internal network). Details of the protective controls that have or will be implemented must be provided.</p>
NW.5	<p><i>Connectivity to other Third Parties</i></p> <p>Details must be provided of connectivity to other third parties that have not been included in the above points. This must include details of any shared components or networks and how data and traffic separation will be enforced along with what protective measures have been implemented.</p>
NW.6	<p><i>Remote Access</i></p> <p>Details must be provided of any remote access systems that are in place that will provide the Contractor's staff with access to systems and/or data that provide a service or are used by the NICS. Details must include:</p> <ul style="list-style-type: none"> • The authentication mechanisms that are in place; • Any data transmission security that is in place; • Protective measures that are in place to safeguard NICS related information on the Contractors staff PCs/laptops; • Usage policies that will be applicable to using the remote access service; and • What protective monitoring measures will be in place.

NICS CODE OF CONNECTION
(Not Protectively Marked)

Ref	Requirement
NW.7	<p><i>Wireless Networking</i></p> <p>Details must be provided of all wireless technology that is being used by the Contractor in support of the NICS systems and/or data. This will include the use of wireless within the hosting, support, operational, site-to-site and working/office environments.</p>
NW.8	<p><i>Wireless Logging</i></p> <p>The wireless access point/s must be configured to log connections including MAC (or equivalent) addresses of connected systems and the time/date. Details must be provided of where these logs will be stored, who will review them, the frequency of the reviews and the length of time that the logs will be retained for.</p>
NW.9	<p><i>Third party devices</i></p> <p>Where the Contractor requires third party devices (e.g. CPE routers or supplied servers/systems) to be connected to the NICS infrastructure (either directly or via a common network such as the PSN or Network NI), NICS must have access to the configuration either directly or as documented.</p>

Comment [BO1]: Should reference to the appropriate CESG Manual be made here.

Security of Communications

Ref	Requirement
NW.10	<p data-bbox="338 369 464 398"><i>Encryption</i></p> <p data-bbox="338 405 1144 546">Where connections are to be established externally, and data is to be exchanged with systems or individuals over public, un-trusted or external networks, the data exchanged must be protected from passive or active interception, including the use of cryptographic protection (e.g. using appropriate encryption mechanisms).</p> <p data-bbox="338 553 1144 636">Details must be provided where the Contractor will be implementing encryption technology for any of the data or voice communications. The information must include details of the</p> <ul data-bbox="379 642 1144 1102" style="list-style-type: none"><li data-bbox="379 642 836 672">• The reason for deploying the devices;<li data-bbox="379 678 735 707">• The devices to be deployed;<li data-bbox="379 714 1144 1102">• Compliance with the requirements stated within the HMG Security Policy Framework and HMG IA Standard IS4 to include at least the following aspects:<ul data-bbox="459 808 1144 1102" style="list-style-type: none"><li data-bbox="459 808 1018 837">○ What level of approval/accreditation they have;<li data-bbox="459 844 863 873">○ Who will manage them and how;<li data-bbox="459 880 1070 909">○ Key management processes to include key loading;<li data-bbox="459 916 1144 972">○ The length of time that the keys will remain valid for and the fallback measures in place should key renewal fail;<li data-bbox="459 978 1144 1034">○ Responsibilities in relation to key material and who will be supplying this; and<li data-bbox="459 1041 1144 1102">○ What additional protective controls will be required for the devices.

NICS CODE OF CONNECTION
(Not Protectively Marked)

Data Exchange

Ref	Requirement
NW.11	<p><i>Data Exchange</i></p> <p>There will be instances where the NICS have a requirement to access data hosted by the Contractor and vice versa. The Contractor must supply information relating to:</p> <ul style="list-style-type: none">• The type of data that will be exchanged;• The direction of data exchange;• What protective measures will be in place to secure the data whilst in transmission; and• The network protocols that will need to be permitted on the perimeter security devices to facilitate this exchange.

Data Exchange to Lower Classified Systems

Ref	Requirement
NW.12	<p><i>Data Exchange across different Protective Markings</i></p> <p>The Contractor must provide details where the NICS data or systems are accessed or stored on a different protectively marked system. This should include instances where the other systems are both higher and lower protectively marked. The assumption should be made that all the NICS data and systems are protectively marked at the RESTRICTED level.</p>

Cross Network Authentication

Ref	Requirement
NW.13	<p><i>Protection of user credentials</i></p> <p>User credentials (i.e. passwords) must be protected in transit to safeguard the security of authentication processes. This can either be achieved using secure authentication techniques that protect the credentials and prevent replay such as challenge-response or cryptography or by securing the underlying traffic through e.g. SSL, SSH or encrypted VPN.</p>
NW.14	<p><i>Authentication of Third Parties</i></p> <p>Wherever connections are to be established from third party users to internal NICS systems, the access must be authenticated with two factor authentication. An audit trail must also be maintained by these systems.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Firewall Requirements

Firewall devices control traffic flows based on a number of factors, including the source and destination network addresses (of individual systems, address ranges or entire subnets) and also the application ports (both TCP and UDP) which denote the type of traffic (e.g. web, mail, Windows) that are permitted in either direction.

The presence of strict controls over the origins and destinations (or network hosts) of the network data flows and the types of protocol permitted are vital to reduce the risk of attack and to prevent all but the required usage of interconnected systems.

This section though not explicit in terms of the configuration that should be applied to the perimeter security devices, should be used as a guideline as to the applicable rulebases.

Ref	Requirement
NC.15	<p><i>Inbound¹ Destination Ports/Traffic</i></p> <p>Inbound network connections must have a defined set of TCP/UDP ports permitted on the perimeter security device.</p> <p>Where possible the destination addresses must be defined to limit access to only specific systems where communication is required.</p> <p>Applications should not be used that require a wide range of port numbers to be permitted through the firewall or where port hopping is utilised.</p>
NC.16	<p><i>Outbound destination ports/traffic</i></p> <p>Where outbound connections are to be supported the ports must be confined to only those individual ports (applications) required by the application.</p>
NC.17	<p><i>Address specification</i></p> <p>When allowing inbound traffic through a perimeter security device/firewall the following order should be used:</p> <ul style="list-style-type: none">• Individual addresses;• Address ranges (within a subnet);• Network subnet (only if all systems on the subnet are required to have access);• Multiple subnets; and• Any source/or destination (only in exceptional instances. Examples include an external facing web server that is accessible to all Internet users. In this instance, it would not be able to restrict the source address). <p>Outbound traffic must explicitly identify the individual address of the NICS hosts/systems requiring external access. Wherever possible the external hosts must also be identified.</p>

¹ This relates to inbound to the NICS

NICS CODE OF CONNECTION
(Not Protectively Marked)

Application Security

The remainder of this section addresses the requirements of applications that will be provided and/or hosted by the **Contractor** to the NICS.

Authentication

Ref	Requirement
AS.1	<p><i>Integrated Authentication</i></p> <p>Where possible, the existing NICS Windows Active Directory authentication should be used to validate the user's identity when accessing an application. This process should be transparent.</p> <p>The Contractor must state the systems they will require access to in order to achieve this and when they are hosting the service, the systems or connectivity that will be required to allow the authentication to take place (i.e. access into the NICS network).</p>
AS.2	<p><i>Dedicated Authentication</i></p> <p>Where AS.1 cannot be accomplished, the Contractor must supply details of the authentication mechanism that will be employed. The information provided must encompass the following:</p> <ul style="list-style-type: none">• The password controls that are available (length, complexity etc.);• The system/application that will be fulfilling this function;• The processes surrounding provisioning new user accounts for the application and the supporting processes for user updates and deletions;• Is the authentication mechanism compliant with the HMG standards (specifically memos 24, 26 and 27); and• Has the solution been evaluated and if so, the level it was evaluated to and the results of the evaluation.
AS.3	<p><i>Authentication of NICS Users</i></p> <p>Where third parties will be providing systems that will reside within the NICS environment, authentication should be established using the NICS users network logon credentials.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Access Control

Ref	Requirement
AS.4	<p><i>System Access Control</i></p> <p>The Contractor must provide details of the access control measures that will be implemented on the operating system of the devices/appliances that will be supporting the NICS. This should also demonstrate how segregation of duties (where relevant) has been implemented.</p>
AS.5	<p><i>Application Access Control</i></p> <p>Where an application is being provided, the Contractor must provide details as to how access control will be implemented within the application. This should include an access matrix and how segregation of duties has been implemented.</p>
AS.6	<p><i>Audit Trail</i></p> <p>Details must be provided of the audit trail that will be maintained that tracks user's activity. The information that must be recorded is:</p> <ul style="list-style-type: none"> • Session start and end time; • Unique user account that was used to logon; • Any administrative activity that was performed; • Failed attempts to logon or access an object; • Where the audit trail information will be stored and the length of time that it can be stored for; and • The mechanisms available to interrogate the audit log. <p>Where additional auditing capabilities are available in excess of that listed above, this should be detailed</p>
AS.7	<p><i>Segregation of Duties/Role Based Access Control</i></p> <p>Details must be provided as to applications capabilities to control access to the data and/or functionality.</p> <p>Details should also be provided of the capability to implement a "read-only" role.</p>
AS.8	<p><i>Administrative Activity</i></p> <p>Details must be provided of the administrative functions that are available and how these can be assigned to users. All users must have their own unique user account.</p>

Operational Security

Data Security

Ref	Requirement
OS.1	<p><i>Data in storage</i></p> <p>Data hosted on behalf of the NICS departments, its staff or otherwise must be given adequate protection when in storage on or off-site or stored on external systems. Where the data is stored on the network, the principle of least privilege must be applied to those who are granted access to it. The Contractor must provide details as to how this be achieved.</p>
OS.2	<p><i>Access to data by third parties</i></p> <p>Where third parties have access to NICS systems for support purposes or otherwise, any access to data they require must be only as directly required by the business needs and access to live and/or sensitive data must be controlled.</p> <p>Live data must not be used for test purposes or extracted from the NICS systems in a meaningful form (i.e. where extracting the data would identify an individual or could lead to a breach of the DPA).</p> <p>Confirmation is required from the Contractor that processes will be implemented to support this requirement.</p>

Patching

Ref	Requirement
OS.3	<p><i>Patch Management</i></p> <p>Details must be provided of the patch management processes that will be adopted by the Contractor for all the devices that they will be hosting and/or managing on behalf of the NICS.</p>
OS.4	<p><i>Testing</i></p> <p>Details are to be provided of the testing processes that are employed by the Contractor prior to patches being distributed.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Ref	Requirement
OS.5	<p><i>Patch Distribution</i></p> <p>Details of the methods that are used by the Contractor to distribute/ implement patches must be provided. This must also include the method that is used to verify the success or otherwise of the installation of the patch.</p> <p>The processes that are in place to roll-back patches that have had an adverse effect must also be detailed.</p> <p>Confirmation must be given that all appropriate service packs and hotfixes are applied. Where it has been decided not to apply such fixes, the NICS must be advised as to why this is the case.</p>

Content Security

This section also incorporates malware, spyware and malicious code.

Ref	Requirement
OS.6	<p><i>Content Security</i></p> <p>Where the service being provided by the Contractor incorporates data feeds or connectivity from systems external to the NICS and the Contractor, content security controls should be implemented (e.g. the scanning of web based content for malware) where appropriate. Details must be provided as to how this will be achieved.</p>
OS.7	<p><i>Anti Virus Provision</i></p> <p>Where the Contractor will be hosting systems that are used by the NICS, details must be provided of the anti virus measures that will be in place, including the method and frequency for applying updated definition files and how the methods/tools that will be in place to monitor the status of the anti virus implementation.</p>

Asset Management

Ref	Requirement
OS.8	<p><i>Asset Register</i></p> <p>Details must be provided by the Contractor as to how hardware and software assets will be recorded that are owned by the NICS but are hosted by the Contractor.</p>

Protective Marking

For the purpose of this code of connection, it should be assumed that all assets will attract a protective marking of RESTRICTED.

NICS CODE OF CONNECTION
(Not Protectively Marked)

Ref	Requirement
OS.9	<p><i>Protective Marking – Hardware</i></p> <p>The Contractor must provide details as to how all IT hardware and associated components that are used in providing a service to the NICS will be protectively marked. This must also include removable media (e.g. CDs, tapes, server disks etc.) including USB devices (such as memory sticks).</p>
OS.10	<p><i>Protective Marking – Paper Material</i></p> <p>Details must be provided by the Contractor how protective marking will be applied to non IT assets (i.e. paper based material). This must also include what provisions will be made for storage of such items.</p>
OS.11	<p><i>Protective Marking – System</i></p> <p>Where the Contractor will be hosting systems/applications on behalf of the NICS, the measures that will be implemented to ensure that the Contractors own staff are aware of the protective marking of the system when they logon should be detailed (e.g. usage policy, logon banner).</p>

Protective Monitoring (Logging)

Ref	Requirement
OS.12	<p><i>Log Collection</i></p> <p>The Contractor must provide details relating to the method/s that will be employed to capture the logging information from the devices and systems that will be used by the NICS. Details of the retention period must also be provided.</p> <p>At a minimum, all systems, servers, perimeter/authentication devices and (where applicable) applications must be capable of logging the following activity:</p> <ul style="list-style-type: none"> • User logon and log off; • Failed log on attempts; • Failed connection attempts; • Administrative accesses/changes; and • Any suspicious activity or any event classified as a security incident by the device/documentation.
OS.13	<p><i>Security Monitoring facilities/subsystems</i></p> <p>Where systems or platforms have enhanced security monitoring facilities or sub-systems these must be enabled or activated to ensure the maximum amount of security related information is available.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Ref	Requirement
OS.14	<p><i>Log Collection / Management</i></p> <p>The following processes must be initiated for all systems that the Contractor is hosting/supporting:</p> <ul style="list-style-type: none"> • Log data created should be centrally collected, preferably in real time, but at least daily; • Log analysis must be undertaken to highlight potential security incidents; • Log data must be archived for a period of at least 6 months; and • A monthly report on log events/incidents must be produced for assessment for IT Assist (or the relevant department if the service is being provided to them directly). Where incidents have been investigated this must also be reported.
OS.15	<p><i>Reporting</i></p> <p>Details must be provided of the reporting mechanisms that will be used to make the NICS aware of any malicious activity that has been detected as well as the processes to inform the Centre for Protection of National Infrastructure(CPNI)</p>

Backup Provisions

Ref	Requirement
OS.16	<p><i>Data Backup</i></p> <p>Details will be provided of the processes and methods that will be used to backup data that the Contractor is hosting on behalf of the NICS. This should include details of the backup solution, the frequency of the backup and details of the data that is being backed up.</p>
OS.17	<p><i>System Backup</i></p> <p>Details will be provided of the processes that will be employed to create, store and use system/image backups (i.e. image builds). Details must also be provided relating to how configuration data will be backed up (e.g. router configurations).</p>
OS.18	<p><i>Restore</i></p> <p>Details must be provided as to how the restore process will work for the above points. This should include the process to support it, the timescales associated with performing restores and the frequency of the testing of the restore processes.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Resilience

Ref	Requirement
OS.19	<p><i>Resilience</i></p> <p>Details must be provided of any single point of failure within the service being proposed by the Contractor. This must include any single point of failure in relation to the Contractor's suppliers. This must encompass all infrastructure and service components.</p>
OS.20	<p><i>Resilience Options</i></p> <p>Where a single point of failure has been identified above, the Contractor must provide options as to how this can be addressed. This must include options for high availability and hot and cold standby.</p>
OS.21	<p><i>Availability</i></p> <p>Based on the requirements defined by NICS and the risk assessment that has been performed, what provisions will be in place to maintain availability of the service/application?</p>

Continuity Arrangements

Ref	Requirement
OS.22	<p><i>Business Continuity</i></p> <p>The Contractor must provide details of the business continuity arrangements that are being proposed. At a minimum, this must include the following:</p> <ul style="list-style-type: none">• Location of sites and distance between them;• Connectivity between sites;• Single points of failure at the DR site and within the intersite connectivity;• The level of continuity provided and any services that will be unavailable;• How the change control process will incorporate business continuity provisions;• The expected length of time to reinstate the service; and• The processes and frequency for testing the Business Continuity plan.

NICS CODE OF CONNECTION
(Not Protectively Marked)

System Management

Ref	Requirement
OS.23	<p><i>System Management</i></p> <p>Where the Contractor will be hosting systems/data on behalf of the NICS, details of the system management and monitoring methods must be provided. This shall include what products and/or tools are used, who will be monitoring them and the type of information that will be captured.</p> <p>Details must be provided of any devices that will not be included within the proposed solution.</p>

Incident Management/Escalation

Ref	Requirement
OS.24	<p><i>Incident Management & Escalation</i></p> <p>Details must be provided of the incident management and escalation processes that the Contractor will apply to the NICS service provision. This should include the specific roles that will be involved within the organisation, how the process will be communicated to the relevant Contractor's staff and how the escalation to the NICS will be undertaken.</p>
OS.25	<p><i>Incident Log</i></p> <p>Details must be provided of the recording mechanism that will be used by the Contractor to capture any incidents along with the action that was taken. This must also include the frequency with which the log will be examined and which role within the Contractor's organisation will have the responsibility to perform this.</p>

Change Control

Ref	Requirement
OS.26	<p><i>Change Control</i></p> <p>The Contractor must supply details of their change control process and how the NICS will be informed of any changes to the environment used to provide a service to them.</p> <p>They should also be included in the change authorisation process.</p> <p>Details must also be included of the testing processes and the back out plans that are employed.</p>

NICS CODE OF CONNECTION
(Not Protectively Marked)

Physical Security

The **Contractor** must provide details as to how the following physical security requirements will be met.

Shared Facilities

Ref	Requirement
PS.1	<i>Physical Security – Secure room</i> NICS systems, network components or systems processing NICS data must be housed in locked rooms/dedicated secure cages to which access controls are in place and visitors are recorded and logged.
PS.2	<i>Physical Security – lockable cabinets/racks</i> Particularly where there is shared access to equipment rooms with other parties or support staff have access to the NICS hosting area who are not supporting the NICS account, the hosted NICS equipment/data must be housed in a lockable cabinet/rack. Cabinets must have a unique lock and the keys must be secured by the Contractor .
PS.3	<i>Patch panel access</i> Access to patch panels and network trunking must be controlled where possible to prevent systems being accidentally or maliciously connected to the hosted NICS network.
PS.4	<i>Labelling of devices/cables/ports</i> All NICS equipment, racks/cabinets, cables, trunking and network ports/floor boxes must be labelled or colour coded to clearly indicate their nature and ownership within the Contractor's hosting environment.
PS.5	<i>Intrusion Detection</i> The Contractor must provide details of what complementary physical security countermeasures are in place to support both protective and reactive monitoring of the hosting facilities used by the NICS.
PS.6	<i>Remote Working</i> Where support will be provided remotely (i.e. away from the Contractor's office location/s), details must be provided of the measures that will be taken to safeguard access to the NICS systems and data.

SECTION 3

Code of Connection for End Users

Introduction

The Network NI (NNI) infrastructure is accredited for RESTRICTED (impact level 3) by the NICS Accreditation Panel. Furthermore protection against integrity and availability problems is provided in accordance with impact levels 3 and 4 respectively.

This Code of Connection describes the security controls that end-user organisations must implement in order to access NNI, not withstanding further security controls relating to the applications hosted at the SSC.

Organisations wishing to connect to NNI are required to:

- Read the Code of Connection
- Comply with the requirements for security controls. *Note provision has been made for end-user organisations to indicate compliance or otherwise*
- Sign the 'commitment statement' at Appendix A
- Return all documentation to the NICS Accreditation Panel

Any questions shall be raised with IT Assist/NNI project office.

Finally it should be noted that the applicability of some security controls depends on the types of sites occupied by end-user organisations (see below for further details).

Background

There are three types of sites;

1. Medium - large sites managed by NICS – and with dedicated communications / server room
2. Small sites managed by NICS – typically with no dedicated server / communications room
3. 'Shared' sites (where NICS has a presence) and typically managed by another party

Security controls – for sites with a dedicated server / communications room

Description	Compliant (and comments)
1. All entrances to the server / communications room shall be secured by a door and locking system which are resistant to an attack by a reasonably determined attacker using portable hand tools.	

NICS CODE OF CONNECTION
(Not Protectively Marked)

2. Any external walls of the server / communications room shall be solid, which excludes stud-partition and glass walls. Walls constructed using brick, blocks and stone are acceptable.	
3. Walls of the server / communication room which are internal to the building:	
<ul style="list-style-type: none"> • For a well protected building – ‘walls constructed using brick, block, stone, stud-partition or ‘toughened’ glass are all acceptable 	
<ul style="list-style-type: none"> • For a ‘poorly’ protected building - walls constructed using brick, block, stone, or ‘toughened’ glass are all acceptable 	
4. Windows within the server / communications room shall be secured to prevent unauthorised access by an attacker using portable hand tools. Suitable security measures include window bars and double glazing.	
5. Unauthorised access to the server / communications room shall not be possible via the ceiling or loft space.	
6. Access to the server / communications room shall be controlled by a mechanism (e.g. swipe card system) that restricts access to everyone apart from named and authorised individuals with ‘Baseline Standard’ clearance (minimum)	
7. Smoke detectors shall be installed in the server / communications room including an alarm system that is audible 24*7.	
8. Fire suppression equipment shall be installed in the server / communications room.	
9. Measures for maintaining a suitable operating environment for the equipment shall be implemented (e.g. air conditioning).	
10. The server / communications room shall not be situated where it may be susceptible to flooding caused by:	
<ul style="list-style-type: none"> ◆ River(s) 	
<ul style="list-style-type: none"> ◆ Sea 	
<ul style="list-style-type: none"> ◆ Rain 	
<ul style="list-style-type: none"> ◆ Plumbing failure (including rooms at any level above the server / communications room) 	
Pipe work (including pipe work above false ceilings and below suspended floors) shall be routed in such a	

NICS CODE OF CONNECTION
(Not Protectively Marked)

manner that if these pipes leak then any discharge will have no impact on any equipment or associated equipment.	
11. Power supplies to the server / communications room shall be adequate (in terms of capacity), reliable and secure (e.g. against accidents or malicious damage).	
12. The end-user organisation shall maintain a list of named individuals, including ancillary staffs, maintenance staffs, and contractors, with authorisation to access the server / communications room. Authorisation shall be based on the individual having:	
<ul style="list-style-type: none"> • A business requirement (ongoing) 	
<ul style="list-style-type: none"> • Baseline standard check 	
13. The server / communications room shall be maintained in a tidy state.	

Security controls – for sites ‘without’ a dedicated server / communications room

For sites without a dedicated server / communications room, or where the controls referred to in the previous section cannot be implemented, the following security controls apply.

Description	Compliant (and comments)
1. A secure cabinet shall be provided to house NNI equipment, which is resistant to an attack by a reasonably determined attacker using portable hand tools	
2. Access to the secure cabinet shall be controlled by a ‘locking’ mechanism that restricts access to everyone apart from named and authorised individuals with ‘Baseline Standard’ clearance (minimum). Furthermore a well-defined and ‘effective’ key management process shall be implemented.	
3. The end-user organisation shall maintain a list of named individuals, including ancillary staffs, maintenance staffs, and contractors, with authorisation to access the secure cabinet. Authorisation shall be based on the individual having:	
<ul style="list-style-type: none"> • A business requirement (ongoing) 	
<ul style="list-style-type: none"> • Baseline standard check 	
4. The secure cabinet shall not be situated where it	

NICS CODE OF CONNECTION
(Not Protectively Marked)

may be susceptible to flooding.	
5. Power supplies to the secure cabinet shall be adequate (in terms of capacity), reliable and secure (e.g. against accidents or malicious damage).	

The next page contains an illustration of the Compliance Statement for connection to Network NI.

COMPLIANCE STATEMENT FOR CONNECTION TO NETWORK NI

This statement needs to be completed and signed by the Departmental Security Officer (or his/her representative) responsible for the system that will be connected to Network NI.

Name of Organisation:

Sites to be connected to NNI (and covered by this compliancy statement)

It is understood and accepted that:

- The organisation shall endeavour to comply with the Code of Connection at all times and shall inform the NICS security authorities should a 'major' non-compliance occur.
- The organisation accepts that failure to comply with the Code of Connection may result in their connection to Network NI being terminated (in extreme circumstances)
- Confirmation of continued compliance shall be required at twelve-monthly intervals.

Post: _____
Name: _____
Signed: _____

Approval to connect to NNI:

Post: On behalf of the NICS Accreditation Panel
Name: _____
Signed: _____