NBI Partnership

Computing
infrastructure
for Science

NBIP Computing
Permit to Work System

Guidance Notes for NBI Supervisors

Document History

Name and date	Comment
P. Fretter 7th February 2015	Replaced Ian Braid with Ian Venn as area supervisor for IFR W206, B30 and B101 first floor data centres.
P. Fretter 13th March 2014	Re-write of PF's original guidance

Related Documents

NBI Data Centre Permit to Work

NBI IT Network Cabling Infrastructure – Permit to Work

NBI Contractors Information Pack *(multiple documents)*
- Fire advice for Contractors working on NBI sites
- Management of Risks Checklist
- Guidance for Lifting Raised Floors
- NBIP General Conditions of Work

Contents

Purpose of the Permit to Work System

The permit to work system was created to ensure risks are identified and managed for all work activities carried out in the Permit controlled areas. Outcomes should be predictable and safe for persons, equipment, running services and data. Additionally the Permit constitutes a written record of contractor activities in the Permit controlled areas.

Prior to attending site to carry out works the contractor must first submit a Risk Assessment and Method Statement (RAMS) to NBIP for approval, thus requiring that works are pre-planned.

The Permit to Work system is intended to be part of a broader Project Managed approach to the planning and organisation of work activities on site, but it can also be operated standalone for *ad-hoc* pieces of work.

The NBIP Facilities and Risk Management department (FaRM) also operate a Permit to Work system. It is a requirement that works to any M&E systems, cabling containment, building or site fabric must be notified to FaRM and the necessary additional Permits obtained before works are allowed to commence.

Scope of the Permit to Work System

The following areas and systems are subject to a mandatory Permit to Work being issued prior to the commencement of works:

- B26 Data Centre
- B101 Ground Floor Data Centre
- B101 First Floor Data Centre
- B30 Data Centre
- IFR W206 Data Centre
- Invasive or disruptive works to Electrical Plant or Supply to a Data Centre or Wiring Closet
- Invasive or disruptive works to HVAC Plant or Supply to a Data Centre or Wiring Closet
- IT wiring closets, premises network cabling, copper or fibre, internal or external.

When is a Permit to Work required

A Permit to Work is required for all disruptive and non-disruptive activities carried out by contractors or other non-NBIP staff in areas covered by the Permit to Work system.

This includes all installation, modification, maintenance and removal activities to all IT systems, cabling, containment, racking, power and cooling. Additionally any works to the building or estate fabric that is deemed likely to impact on, or pose a risk to, IT systems and services.

When is a Permit to Work not required

Tours and inspections escorted by a member of NBIP Computing and/or FaRM

Works carried out by NBIP Computing and NBIP FaRM do not normally require a Permit to Work, but it is expected that a Risk Assessment and Method Statement is produced and authorised by Computing and/or FaRM as appropriate prior to works commencing.

Outline of the Process

Authority for works to take place must be sought from an IT Area Authoriser.

A nominated IT Area Supervisor, who understands the nature of the works and has been trained to assess RAMS, will issue the actual IT Permit to Work.

See *Appendix 1* for a list of IT Area Authorisers and Supervisors

All works to M&E, building fabric or within external ducting will require additional permission from a FaRM supervisor. There may also be a requirement for FaRM to issue a Permit to Work.

1. A work activity is identified to take place in a Permit Controlled area	✓
2. Authorisation for the works is sought from the relevant Authoriser (*see Appendix 1*), and also from FaRM where works to any M&E systems, cabling containment, building or site fabric is involved.	✓
3. Area Supervisor issues the “NBI IT Contractor Guidance Information Pack” to the Contractor. FaRM may require to issue additional guidance.	✓
4. Contractor issues RAMS to Area Supervisor (and FaRM) for approval in advance of works taking place	✓
5. Area Supervisors and FaRM review the RAMS, in line with the guidance notes	✓
6. NBIP IT, FaRM and Contractor agree RAMS	✓
7. Contractor arrives on site	✓
8. Area Supervisor delivers a Pre-Start Briefing to Contractor	✓
9. Area Supervisor and Contractor fill in the Permit to Work form(s)	✓
10. Area Supervisor issues Permit(s) to Work	✓
11. Contractor carries out works.	✓
12. Area Supervisor (and FaRM) inspects completed works	✓
13. Permit is signed off by Area Supervisor and works are either accepted or referred to the Contractor for remediation	✓

Reviewing a Risk Assessment and Method Statement (RAMS)

It is the responsibility of the Contractor or other persons carrying out the works to prepare and submit a RAMS to NBIP for approval, and in consideration of the documentation provided in the NBI Contractors Information Pack. A nominated NBIP Area Supervisor will then review the RAMS and, if necessary, enter into a discussion with the contractor to ensure all the required information has been provided before the Permit is issued.

All reputable contractors will be familiar with Risk Assessments and Method Statements, and will often have their *pro-forma* documentation which will be edited to suit a particular work activity. Some organisations will refer to this as a Statement of Work (SoW), however the contents and meaning are the same.

Risk Assessment

An assessment must be made of the potential risks to persons as well as assets such as equipment, running services and data. The assessment must include controls to manage the risks associated with the planned activities. Refer to the "Management of Risks Checklist" document for a general guide to risks in this area. Additional risks will also be associated with a Contractor's own working practices and tools or equipment.

There are two components to a risk: Severity and Likelihood

Risks are to be mitigated by introducing controls into the working methods. The aim of a risk control is to reduce the Severity and Likelihood to an acceptable level.

In addition to the physical risks to persons and equipment, consider carefully any inherent risks to data or service during software installation, upgrade or configuration work, or any works involving the movement or modification of stored data.

Method Statement

This should be in the form of an itemised, chronological list of the tasks to be performed and the methods employed. This should include processes or procedures for all tasks of hardware or software inspection, installation, modification and removal.

Straightforward and low risk activities can usually be addressed with a succinct RAMS. Complex and/or riskier activities will require a more comprehensive RAMS document.

It is important to consider the potential risks to service availability and data integrity. IT hardware and software installation or modification works will often require a Rollback Plan to be included in the Method Statement, in case there is an insurmountable problem occurs and it is necessary to restore systems or services to the previous known working state.

If you do not fully understand the nature and implications of the proposed work activities, please ask other NBIP staff members for advice or assistance.

Some specific activities undertaken will be outside of the normal IT staff skillset, and may be subject to HSE legislation and/or guidance. For example, electrical works, working at height, use of power tools, confined spaces, hot works etc. These will usually require additional permission and supervision from FaRM.

If in doubt, ask.

Choosing an appropriate Permit to Work form

All works within, or affecting, Data Centres should be dealt with using the following form:

NBI Data Centre Permit to Work

All works to IT network cabling (copper or fibre), cabinetry, internal/external containment, and ductwork should be dealt with using the following form:

NBI IT Network Cabling Infrastructure – Permit to Work

Works involving cabling/containment etc that also require access to a Data Centre will also require an **NBI Data Centre Permit to Work**

All works to mechanical and electrical systems, building fabric, cable containment, external ducting etc will require an additional Permit to Work from FaRM.

When is a RAMS document not required

There are occasions when no actual works will take place in a given area, for example when

- Visually inspecting equipment
- Delivering or removing loose items (not in racks)

Under these circumstances there no perceived additional risks and the activity should be clearly written in Section 1 "Purpose of Works" and marked as Exempt to "Acceptable RAMS supplied?"

Delivering a Pre-Start Briefing to a Contractor

The pre-start briefing is to be conducted by the IT Area Supervisor and, where applicable, with a FaRM representative and the local Laboratory Manager.

- Local Fire evacuation procedure
- Location of toilets, smoking areas and other permitted facilities
- Request contact phone numbers of Contractor staff on site
- Provide contact names and phone numbers of the IT Area Supervisor and other persons responsible for the works (e.g. FaRM).
- Provide contact name and phone number of local Lab Manager (if applicable)
- Notice of relevant adjacent works and routine activities
- Other local procedures or notifications as required

Issuing and managing the Permit to Work forms

The Area Supervisor will issue and manage the Permit to Work as follows:

1. Contractor/Works Information

- Enter the contractor details, including any NBIP or contractor reference/job numbers.
- **[NBI IT Network Cabling Permit]** If the contractor is not already approved by NBIP Computing, works are not permitted to proceed.
- Enter a brief description of the works. A fuller description will be required in the RAMS
- Review the RAMS as per the "Guidance notes for Preparing and Reviewing RAMS" document
- Ensure the contractor has been issued with appropriate site rules and documentation and is fully aware of their content.
- Deliver a short briefing on the necessary fire evacuation procedure

2. Location of Works

- **[NBI IT Network Cabling Permit]** The route and/or multiple locations of works should be briefly described.
- **[NBI Data Centre Permit]** Tick the Data Centre(s) which will be the location of the works.
- Works to M&E systems, cabling containment, building or site fabric will require additional Permits from FaRM. Ensure these have been agreed and issued before works commence.

3. Permit to Work

- Sign and date this section to attest that all the above requirements have been met and that it is permitted for works to proceed.
- Attach a printed copy of the RAMS to the Permit to Work
- File the printed Permit to Work and RAMS in the appropriate ring binder in Computing
- **The Permit to Work and RAMS documents are available for inspection by NBIP and the Contractor at all times.**

4. Completion of Works

- Sign and date this section to attest that all works have (ideally) been carried out as per the agreed RAMS, or that works have been unsatisfactory and will be referred for management and the contractor to resolve.

IT Area Authoriser Responsibilities

- Provides authority for the works to proceed, taking into account cost, inconveniences and interactions with adjacent work.
- Authorises the Area Supervisor to obtain RAMS, issue a Permit to Work and supervise the works.
- Receives feedback and complaints from the Contractor and NBIP staff
- Resolves queries and disputes with the Contractor's management and/or NBIP staff
- For fully Project Managed works, appropriate authority can be delegated to the NBIP FaRM Project Manager as required.

IT Area Supervisor Responsibilities

- Checking that authority has been given for the works to proceed *(see Appendix 1)*
- Informing FaRM of activities for which they may require notice and/or to issue an additional Permit to Work
- Assessing RAMS
- Issuing Permit to Work and placing in appropriate ring binder
- Ensure the Contractor is signed in at reception and carrying a visitor badge
- Delivering a Pre-Start Briefing to the contractor prior to works commencing
- Ensure the Contractor is escorted to the work location for the start of works.
- Introducing the contractor to the local Laboratory Manager (if appropriate)
- Periodically visit the works to check the contractor is not obstructed in their activities and that they are working in accordance with the agreed RAMS.
- Where the agreed RAMS is clearly not being observed and new or elevated risks are perceived, the works may need to be halted temporarily while the situation is reviewed.
- Ensure that the contractor reports to you each day, prior to commencing works and again before leaving site.
- Check the completed works as per the agreed RAMS
- Ensuring that all issued security cards, keys, PPE etc are returned.
- Signing the completion of the Permit to Work

Appendices

Appendix 1 - List of IT Area Authorisers and Supervisors

Permit Controlled Area	Authority for works to proceed required from	IT Area Supervisors
IT premises network cabling, copper or fibre, internal or external. All associated containment and ductwork.	Ian Venn	Ian Venn Laurence Bartrum Mohammed Imran
NBI IT wiring closets, or the power/cooling systems associated with them	Ian Venn	Ian Venn Laurence Bartrum Mohammed Imran
B26 Data Centre	Paul Fretter	Paul Fretter Chris Bridson Adam Carrgilson Michael Burrell
B101 Ground Floor Data Centre	Paul Fretter	Paul Fretter Chris Bridson Adam Carrgilson Michael Burrell
B101 First Floor Data Centre	Ian Venn	Ian Venn Laurence Bartrum Mohammed Imran
B30 Data Centre	Ian Venn	Ian Venn Laurence Bartrum Mohammed Imran
IFR W206 Data Centre	Ian Venn	Ian Venn Laurence Bartrum Mohammed Imran

Appendix 2 – Sample Risk Assessment and Method Statement

(This is a very simple example. For complex installations please contact an Area Supervisor for advice)

TASK: Replace faulty hard drive in data storage system in B26 Data Centre

RISK ASSESSMENT

Risk	Impact	Person or Asset	Control
Excessive noise levels	Hearing damage	Person	PPE. Ear defenders with minimum SNR=30 will be worn at all times
Drive not marked ready for removal	Loss of data	Asset	Check drive is already 'failed' out of cluster before removal
Removing incorrect drive.	Loss of data	Asset	Double check node and drive number before removal

METHOD STATEMENT

1. Loan PPE (ear defenders) from Computing G03 office
2. Double check drive has been 'failed' out of the cluster by logging into the OneFS GUI
3. Double check the node and drive number as per the Isilon case No. and the details in the GUI
4. Enter Data Centre whilst wearing PPE , open rack and locate Isilon node and drive
5. Check drive access indicator is quiesced
6. Remove faulty drive
7. Insert new drive and close rack door
8. Login to OneFS GUI and check firmware level on drive. Upgrade if necessary.
9. Run drive self-tests
10. Use OneFS GUI to join drive back into cluster
11. Check drive is joined into cluster and demonstrate to customer
12. Pack failed drive into packaging from new drive and label for courier return