VPN Access for Businesses

Business Details (3rd party support and contractors) (Please print clearly)

|  |  |
| --- | --- |
| Business Name |  |
| Manager’s Name |  |
| Position | Role: |
| Business Number | Bus:  Mbl: |
| E-mail Address | Bus: |

External VPN Information (External to University of Derby only)

|  |  |  |  |
| --- | --- | --- | --- |
| Provided a list of what you need access to | Details: | | |
| What ports are required open? |  | | |
| When is the VPN access required? | Start Date: | How long is the connection needed? | End Date: |

Authorisation (Unauthorised applications cannot be processed).

|  |  |  |  |
| --- | --- | --- | --- |
| By signing this form I agree that this is the access required for this account. | | Call # |  |
| Project Manager Name | Name:  Sig: | Date |  |
| System Owner’s Name | Name:  Sig: | Date |  |

When you have completed this form, please have the Project Manager sign it.

Scan this form and pass to the ITS Service Centre (B201) or email to ITServiceCentre@derby.ac.uk.

Note if the form is not fully completed or authorized the form will be returned.

**Instructions on how to VPN in to the University**

We recommend that you use Cisco AnyConnect client through the University of Derby.

VPN Portal information required:

If you do not have a client:

1. From a browser type in <https://vpn.derby.ac.uk/UoD-Contractor>
2. Enter your username and password provided
3. Select Start AnyConnect Mobility Client
4. Start the Cisco AnyConnect client located on your desktop.

If you have a client:

1. Start the Cisco AnyConnect client located on your desktop
2. Enter your username and password provided.

**Limitations**

The following limitations will apply to VPN clients connecting to the university. Such machines will:

Have no access to their local network or the internet whilst the client is connected

Other than access that would be granted to any machine on the internet, have only access to specified equipment using specified services.

Have their access logged, and these logs kept for six months

**Support**

If the supplied VPN fails, a job must be raised initially with the IT Service Centre to check passwords, and then passed to DNC if necessary to check the VPN itself.

**VIRTUAL PRIVATE NETWORK (VPN) AGREEMENT**

**TERMS AND CONDITIONS**

Upon signing the Virtual Private Network (VPN) request form, you agree and accept the following terms and conditions.

**1.1 Rights to Use Network Connection**

The designated business may only use the Network Connection for business purposes as outlined by the **Third Party Connection Request – Information Requirements Document.**

**1.2 Network Security**

2.1 The designated business will allow only its employees approved in advance by the University of Derby “Authorized Company Employees”) to access the Network Connection. The designated business shall be solely responsible for ensuring that Authorized Company Employees are not security risks, and upon the University of Derby’s request, the business will provide any information reasonably necessary for the University of Derby to evaluate security issues relating to any Authorized Company Employee.

2.2 The designated business will promptly notify the University of Derby whenever any Authorized Company Employee leaves their employment.

2.3 Each party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that (a) such party’s use of the Network Connection is secure and is used only for authorised purposes, and (b) such party’s business records and data are protected against improper access, use, loss alteration or destruction.

**1.3 Requests for VPN Access**

To be completed by the individual. Authorisation for VPN access must be approved by the project manager and System owner. Please submit the completed form to the IT Service Centre who will contact you once you have been granted remote access and will send you instructions on how to access the systems remotely.