Policy and Procedure for Providing Suppliers with Remote Access to IT Systems and Services

Purpose

Where an external party provides support for either all or part of an IT system/service it will from time to time be necessary to allow that supplier to have remote access to that service for support purposes. This can relate to production platforms and/or preproduction platforms, e.g. regarding test or development. Suppliers will often make it a requirement of the support contract that such access is provided.

Scope of application

The policy applies to all systems and services hosted within the University.

Policy

There must be a balance between allowing the service to be effectively and efficiently supported and ensuring the security, particularly the information security and system integrity, of the University. Accordingly, the following items of policy apply in these cases.

1. The supplier and their staff must comply with the University Policy on the Use of Computing Facilities and Resources.

2. If the system being supported contains information that is confidential, sensitive or of commercial value, the supplier must have signed a non-disclosure agreement (or have equivalent contractual obligations) even if it is not intended that the supplier will have access to that information.

3. Access to a university service will only be provided for the minimal period of time necessary and will never be left open indefinitely. Normally, access will be given when a particular support issue has arisen and will be closed once that problem has been solved. For long term support issues, access will normally not be left open over night or over a weekend. The only exception would be where there was an arrangement agreed for remote service monitoring. At the end of an implementation project, access provided to allow suppliers to build the system must be removed.

4. All remote access by suppliers must be logged on the appropriate helpdesk or call handling software (e.g. LanDesk). Often a call will already have been logged as most remote access by suppliers will be as a result of an incident or a change which has been already logged.

5. Data contained within a service must never be updated by the supplier without the express permission of the relevant data custodian within the University, and a detail record must be made of all such changes and included in the call logging software.

6. The supplier must have good information security practices, including having virus protection on PCs, ensuring that their equipment is patched, and that they have appropriate firewalls enabled.

7. The mechanisms for achieving remote access must be agreed with the technical staff of the University involved in its support. Ensuring the information security of the University must be of paramount concern when agreeing such mechanisms.

8. All Data Protection legislation and requirements must be compiled with.

9. Under normal circumstance, the supplier should not be able to access information that is confidential, sensitive, or of commercially valuable; however, in the event that this proves essential the relevant data custodian must have given express permission for this to occur.

Procedure

1. At the end of any implementation project any long term remote access provided to suppliers, including access to test and development systems, should be removed.
2. Even where a system or service is virtually 100% supported by an external party, there must be at least one technical department with assigned responsibility for that system within the University.
3. It must be agreed between the management of the technical staff who support the system and the management of the “business” staff who will maintain the information it contains, who the “data custodian” is for that service. This is the person who would give permission for the supplier to access any confidential, sensitive, or commercially valuable information, or to have any data updates performed by the supplier.
4. Technical mechanisms for providing remote access should be agreed, implemented, and tested with the supplier and data custodian. Normally it should be possible to provide remote access to the supplier within three working hours of the request being made.

Systems Hosted outside of the University

The above procedure only applies to systems hosted within the University. Where the system is hosted outside of the University, the department placing the contract must ensure sufficient controls within that contract for the management of the information it contains, retaining sufficient and effective information security for the University’s need, and that all data protection requirements and legislation are complied with. When considering ensuring sufficient and effective information security requirements it is important to consider:

- Sufficient access to the information contained in the system for the University and its staff, including the ability to get reports for the system and to create system to system interfaces.

- The integrity of the information contained in the system, including ensuring that it can be kept up to date, that audit trails of updates exist, and system interrogation, when appropriate, and that the security is in place to ensure that information cannot be updated incorrectly or inappropriately.

- That appropriate levels of confidentiality are maintained.