# Guidance Note

# Contractor access to University of Aberdeen IT Systems

## Introduction

Contractors may be engaged to install, operate and support IT Systems belonging to the University. This note provides guidance on the interpretation of the University Information Security Policy and other policies in such circumstances.

## Summary

- All contracts must have a clause requiring compliance with the University Information Security Policy.
- If contractor access is to be supervised then the persons undertaking the supervision must have an appropriate skill level.
- It is the IT Services Service Owner and/or the Business Owner's responsibility to agree and authorise contractor access and any associated procedures.
- An effective process must be established to ensure contractor's accounts are closed or handed over when the contract ends.
- A record of contractor authorisations is to be kept.
- The contractor must provide points of contact where security issues can be raised.

## Scope

There are many scenarios where work is undertaken on University systems by people not directly employed by the University. This document covers only those scenarios where work is undertaken on University owned IT Systems, it does not cover those scenarios where the contractor owns and fully manages the IT System and is providing a service e.g. Office 365.

## Definitions

| | |
|---|---|
| Contractor | External suppliers who are contracted to supply goods or services to the University. This can be an individual or an organisation of several individuals. |
| Access Level | The level of access permitted to the IT System. Five broad levels are defined:<br>• Public (any unregistered user)<br>• User (any registered user with no special rights to the application or data)<br>• Application Administrator (full access to the application and data)<br>• System Administrator (full access to the host server)<br>• Domain Administrator (full access to domain entities) |
| Limited access | Contractor requires UoA to explicitly allow access to the IT System, for a specified time limited period. |
| Unlimited access | Contractor may access the IT System at any time without reference to UoA. |
| Supervised access | Access by the contractor is 'watched over' by another party so as to ensure |

| | |
|---|---|
| | they only access those systems necessary and do nothing untoward. |
| Unsupervised access | Contractor may undertake tasks without supervision, at whatever access level has been permitted |

## Discussion

Contractors are typically engaged to:

1. Undertake a specific task, usually short term contract (days). Typically this might be to install and commission a system but could be to deal with a specific issue.
2. Provide 3rd line support, usually on annual contract (years). Typically called to deal with issues that can't dealt with by IT Services staff.
3. Provide 1st and 2nd line support, usually on annual contract (years). Typically contacted by users out with IT Services to undertake all support tasks.
4. Undertake the daily operation of the system (may also include support tasks), usually on annual contract (years). Typically performing routine tasks monitoring of the system and interacting with system users directly.

The requirements for granting contractor access to University IT Systems are the same as those for granting access to University employees, that is compliance with the University Information Security Policy (ISP) and its associated policies. However, contractors and their staff will often not have the same processes as the University and may not understand the sensitivity of University data; therefore their compliance should not be presumed. Some of the key points are:

- University employees are required to comply with the ISP, contracts with suppliers shall contain clauses requiring them to do likewise, along with penalties for not doing so.
- University employees may have received training on the security aspects of the system and understand the sensitivity of the information it contains.
- Contractors are likely to be working for several organisations; they must not disclose University of Aberdeen information to third parties without explicit permission.
- Contracts are with contractors' organisations; where there is a breach of contract it is the organisation, rather than the individual, that will be held to account.
- Contractors are not in the HR System; therefore accounts issued to them will not automatically be closed when the contract ends. An effective process for closing (or handing over) contractor accounts, tied to the end of the contract, should be established. If there is a change of contractor performing the same function the account may be handed to the new contractor. In such cases the password must be changed and a record kept of the date and time of the handover.
- Contractor's access rights may be atypical; a record of authorisations (including access level and whether access is limited and/or supervised) is to be kept.

Whether access to IT Systems by contractors should be **limited** or **unlimited** and whether such access should be **supervised** or **unsupervised** should be decided by the 'manager responsible for the system'. In reaching a decision the following points should be considered:

- The sensitivity of the information the contractor may have access to.
- The level of access required.

- If the level of access required allows access to systems not directly included in the scope of work.
- The relationship the University has with the contractor.
- The need for urgent out of hours access by the contractor, e.g. if they are to provide 24/7 support.
- The availability of a supervisor with the appropriate skill level. If the contractor is undertaking tasks that the supervisor has no understanding of then supervision is of little value.
- The scenario for which access is required. It is unlikely that a contractor would be able to effectively undertake daily operation of a system where limited and supervised access has been imposed.

The 'manager responsible for the system' should also consider and decide the procedure for contractors to access the system including if any special arrangements are necessary, such as two factor authentication.

Routine remote access to University systems by contractors should be through the UoA approved secure mechanisms, currently the SSL VPN and LogMeIn. In the exceptional circumstances that another method is required, this must be approved in advance by Head of Infrastructure Management.

Contractor access should be treated the same whether

- They are onsite or offsite.
- They are using a University device (e.g. PC) or their own (e.g. laptop).

There may be occasions where contractors undertake tasks using a userID not specifically issued to them (e.g. someone 'logs in' to the system then hands the terminal over to the contractor so that they can install software). In such cases all access must be supervised.

Care should be taken to ensure contractors are not inadvertently issued with credentials (userID and password) for accounts with special privileges, e.g. Service accounts ('srv' accounts). Where this is necessary for the task, the password should be changed on completion of the work.

Care should be taken to ensure that only work covered by the contract is undertaken by the contractor, this requires the contract to clearly state Scope of Works. Any changes or additional work must be documented and agreed as a change of scope.

The RFC process should be followed as normal; the fact that the work is being undertaken by a contractor is not in itself justification for changes being Urgent or Emergency.

Security or other issues may occur during or as a result of contractors undertaking work on a system. It is important that we are able to contact the contractor's organisation so that these can be dealt with. A point of contact and second escalation point must be available so that issues can be raised and dealt with in a timely manner.

## Policy

The relevant clauses in the University of Aberdeen Information Security Policy are:

*5.1 External suppliers who are contracted to supply goods or services to the University should, as appropriate, be informed of the University's Information Security policy and may be required to agree to observe that policy. A summary of the Information Security Policy will be provided to any such supplier, prior to any supply of services. The University may require external suppliers of services to sign a non-disclosure agreement to protect its information assets.*

Where the goods or services relate to IT Systems there must be a clause in the contract requiring compliance with the University Security Policy. Where contractors will have access to University data the clause should explicitly state that such data should not be removed from University Systems unless explicitly agreed and then only if the terms of that agreement are complied with.

*9.1 Procedures for the registration and de-registration of users and for managing access to information systems shall ensure that users' access rights match their authorisations.* ***Users shall have a unique identifier (user ID) for their personal and sole use for access to University information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason.*** *Password management procedures shall ensure the implementation of the requirements of the Information Security policies and assist both staff and students in complying with best practice guidelines.*

This should not be interpreted to mean that 'each individual working for the contractor must have their own personal userID'. Usually it will be the contractor (organisation) that will be held to account rather than the individual for any infractions. The University manager responsible for the system should agree with the contractor how many userIDs are required for each contract. This in no way removes any right the University may have to take legal action against individuals.

*9.3 Access to all systems must be authorised by the manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted. Users' access rights must be adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff or students leave the University.*

For most IT Systems the "manager responsible" will be the **IT Services Service Owner** and/or the **Business Owner** of the Service. It is their responsibility to agree and authorise any contractor access and agree what level of access and degree of supervision is required.