Staff access to key corporate applications policy

Policy Statement

An important aspect of maintaining the security and safety of the University's data is to ensure that only users with the correct authorisation have access to the data. The University has an established and documented process to set up access to the network, corporate applications and IT services. Users request access which is reviewed and approved by their line manager:

- the IS Service Desk team sets up access to the network and IT services,
- system administration teams set up access on corporate applications after authorisation by the service owner or their representative.

Access to the network and IT services is revoked by IS on receiving of leavers information through an overnight interface between the HR system and the University's identity infrastructure. This control provides a degree of protection for many corporate applications as access is limited to the network and authentication is handled via the Kent IT account.

This policy sets out the requirements on departments who are using systems that are not fully integrated with the university's identity infrastructure (such as cloud-based, SaaS, or some locally-hosted applications).

The policy applies to all departments that are responsible for key corporate applications – i.e. those applications that deal with personal data and/or financial probity.

Definitions

The following definitions are used in this policy:

Cloud-based service:	Applications hosted outside of the University's data centre(s)
IdM:	Identity Management
Key corporate applications:	Applications that deal with personal data and/or financial probity
SaaS:	Software as a Service
Service Owner:	The department that is the owner of the service/system. This should be a named individual.

Aim

This policy aims to ensure that the university has a robust process for the timely removal/disabling of user IDs of staff that have left the University or have changed role for key corporate applications that are not automatically protected by integration with the University's identity infrastructure.

Timescale

Service owners should ensure that the systems that they are responsible for do not contain user IDs for staff that have left the university or have changed role and no longer need access. This should be done in a timely fashion to ensure that there is no risk of unauthorised access to or modification of data.

Fully integrated

Systems that are integrated with the University's identity infrastructure will automatically benefit from the process that runs an overnight interface between the HR system and the central identity infrastructure. The timing of this process means that access is normally revoked within 24 hours of a change happening.

Partially integrated

Some systems are partially integrated with the University's identity infrastructure. For example, the finance system is hosted within the university's data centre and is only accessible from within the university's network by those with a Kent IT account and a separate system-specific user account. In order to keep the user account systems in sync, the staff leavers listing (from the HR system) is automatically compared with a list of finance system users on a daily basis – providing a highlight to the finance system administration team where access need to be manually withdrawn.

No integration

Systems that are not integrated with the University's identity infrastructure systems have an entirely separate user account mechanism. Access to the system should be revoked within the same timeframe as for that achieved above – i.e. 24 hours where possible.

Procedure

It is the responsibility of the Service Owner to ensure that access to their systems is revoked for staff leaving or changing their responsibility. The following may help:

- An automated overnight process already runs on the HR system to identify staff leavers. A report can automatically be sent [NB: details of this required]
- Ensure that processes that are used when staff leave (leaver forms, exit interviews, etc) incorporate a check on which systems need to have access revoked.
- Conduct an annual review of users on the systems to ascertain that the correct users have access to the correct part of the system
- Explore whether full integration with the University's identity infrastructure is a possibility.

Support and advice

Service Owners can seek support and advice from Information Services on ensuring that their use of IT systems complies with this policy. Please raise a ticket by simply sending an email to the helpdesk@kent.ac.uk address.

Many modern cloud-based systems can provide some form of integration with the University's identity infrastructure. The main system that is used by the University to facilitate this is called 'federated access' and uses SAML 2.0 technology standards. Contact your supplier and ask them if they can support this mechanism. More information available here: www.kent.ac.uk/itservices/ [page-needs-to-be-created].

Information Services will provide advice and support for the tender/procurement process.

Policy approved	ITUP
Policy discussed	ISB
Date of publication	July 2015
Review date:	+ 1 year from above