

---

## 1 Introduction

The Computer Centre may provide a member of staff who requires elevated access privileges with an additional network account from which such actions may be carried out in a standard auditable way. Examples of such an account would be a *technical administrator account* (or *ADM account*) or a database administrator account (or *DBA account*). Where this policy refers to an extended-privilege account in general, it will be called an *EP account*. By this means, if an EP account-holder's standard network account becomes compromised, then these additional privileges are not also compromised. It also means that this additional access can be quickly stopped (by disabling the EP account) without disabling the standard account (which would result in the staff member being cut off from e-mail, etc.). An EP account may allow the account-holder to undertake such tasks (as appropriate to the account type) as

- adding a PC to the domain.
- logging onto a PC as a local administrator.
- logging onto a server as a local administrator.
- editing a group policy within a specific organisational unit (OU).
- acting as a domain administrator.
- performing high-level database administrative operations (e.g., creation, shutdown or recovery, and execution of OS system commands).
- ability to access fully a database's base tables, views and data dictionary.
- ability to access to a database instance even when the database is not open.
- ability to change a database's security settings.

An EP account only has the additional access to allow that staff member to undertake the extra tasks which require the privileges associated with the account; they do not have e-mail, filestore space or roaming profiles.

An EP account will have appropriate audit-trail assurance built into its parameters. This will allow monitoring and investigation of account use, covering such areas as accountability, deterrence, management notification, and activity audit.

This policy covers *all* EP accounts, whether issued to a member of staff in the Computer Centre or in any other unit of the University.

## 2 Requesting an EP account

Each EP account requires sponsorship by a senior staff member before being considered for creation. This will normally be the Team Leader of the requester's IT servicer, but may be an appropriately senior line manager if there is no Team Leader. The sponsor must ensure that the permissions being requested are reasonable, and will be the point of confirmation that the EP account is still necessary for operational purposes at periodic review. The sponsor must inform the Computer Centre immediately the EP account is no longer required to be held by the account-holder, by e-mail to [computing-support@brunel.ac.uk](mailto:computing-support@brunel.ac.uk) in the first instance.

### 3 Approving and creating an EP account

An EP account will be considered and (if approved) subsequently created under the authority of the Systems Manager of the Computer Centre, who may delegate parts of the process appropriately. For example, authorities regarding ADM accounts may be devolved to a member of the Systems team; for DBA accounts, authority may be devolved to the principal Database Administrator within the Computer Centre.

In order to avoid any potential conflict of interest, the approval of an EP account for any member of the Systems team must be endorsed *a priori* by the Assistant Director (Technical Services) of the Computer Centre or by her/his line manager. Similarly, the approval of a DBA account for the principal Database Administrator must be endorsed *a priori* by the Assistant Director (Governance and Corporate Services) within the Computer Centre, or by his/her line manager.

### 4 Using an EP account

An EP account is not simply another account: the privileges granted for use imply a greater degree of trust in the account-holder. For this reason, the scope of use of an EP account must be more stringent than for a standard account.

The EP account must have a strong and secure password. As for all accounts, this password must not be shared with anyone else. Failure to abide by this instruction will be considered a serious lapse of discipline.

The EP account must be used only for the tasks approved at the time of the account's creation. Any abuse of this account may result in it being disabled with no warning to the account-holder, who may be subject to disciplinary proceedings.

The use (or attempted use) of an EP account by anyone other than the account-holder (including the holder of another EP account) may result in disciplinary proceedings.

The EP account should only be active during the time needed to carry out the required tasks. Leaving an EP account logged into a PC or server beyond such minimum time will be considered a serious lapse of discipline.

Each member of staff who carries an EP account will automatically be added to the Computing Contacts mailing list and to that staff group. This list/group is a primary means of communication regarding the University's IT service to key IT staff.

The use of an EP account is subject to all other policies, rules and regulations of the University: <https://intra.brunel.ac.uk/s/cc/Pages/Policies.aspx> contains those policies managed by the Computer Centre.

### 5 EP account review

Because of the heightened privileges accorded to an EP account-holder, there must be clear procedures for review of an EP account. The principal reviewer of an EP account will be the account sponsor, working in conjunction with the Systems Manager within the Computer Centre (who has overall authority in these matters) and, in the case of a DBA account, with the principal Database Administrator within the Computer Centre.

There will be an overall periodic review of EP accounts: on an annual basis, each sponsor will be required to confirm, for each EP account under her/his sponsorship, that the account is still necessary

for operational purposes. The sponsor will have twenty working days to confirm an account, after which it will be disabled.

If the holder of an EP account changes role in any way, a particular review will be triggered. It is the joint and several responsibility of the sponsor and the account-holder to inform the Computer Centre (by e-mail to [computing-support@brunel.ac.uk](mailto:computing-support@brunel.ac.uk) in the first instance) of any such change of role as soon as such change is known to either party (*i.e.*, without waiting for the actual change date). The Computer Centre will also take notification of a change of role from HR as a trigger for a review.

## 6 EP account disablement

Because of the enhanced privileges accorded to an EP account, the Systems Manager within the Computer Centre (or a nominated deputy) has the authority to disable any EP account at any time, without notice, if he/she has reasonable cause to suspect a potential compromise of the integrity of the University's IT service, or any part thereof.

In the event of the sudden departure of a holder of an EP account, it is the duty of the sponsor to inform the Computer Centre (by e-mail to [computing-support@brunel.ac.uk](mailto:computing-support@brunel.ac.uk) in the first instance) immediately, and the account will be disabled forthwith. The Computer Centre will also take notification from HR of such a departure as a trigger for disablement.