

## Username & password policy guidelines for Athens accounts

### 1. Introduction

The following guidelines reflect the policies that Eduserv Athens recommends for the issuing and management of usernames and passwords enabled for access to Athens protected resources. These recommendations apply to Athens accounts created in Athens using the Athens Administration Interface, called classic Athens; and also to local organisation accounts that are enabled for access to Athens protected resources using Athens Local Authentication facilities as described at [http://www.athensams.net/upload/resources/doc/athens/userpasswordpolicy\\_audit.doc](http://www.athensams.net/upload/resources/doc/athens/userpasswordpolicy_audit.doc).

New organisations registering for Athens, and organisations registering a Local Authentication system will be required to complete the Eduserv Athens Username Password Policy questionnaire at <URL>. Based on the answers provided, Eduserv Athens will determine whether the policy is appropriate for access to Athens enabled resources.

If you have any questions about these Guidelines, please contact the Eduserv Athens Service Desk on +44 1225 474333 or email [athenshelp@eduserv.org.uk](mailto:athenshelp@eduserv.org.uk).

### 2. Issuing of Athens enabled accounts

The organisation should have a clear policy and documented procedures describing under what conditions accounts should be issued. These procedures should be implemented by suitably trained staff.

Each account should have an associated set of Athens access rights, which should take account of the licence conditions for each Athens protected resource. For some organisations one set of access rights may be sufficient, for others there may be clear categories of users with different sets of access rights. For instance, retired members of staff may be entitled to access some resources, walk-in users a different set of resources.

There should be a regular review of these access rights to ensure that access rights are adjusted appropriately and in a timely manner whenever there is a change in resource licence conditions or user access rights. A user may change their role, or may leave the organisation. Accounts for individuals who leave the organisation should be deleted promptly. The access right review period should not be more than one year.

All users should have a unique account for their personal and sole use.

Users should be made aware that this account is strictly confidential; should not be shared with anyone else and should only be used for the purpose for which it was issued.

Shared Athens accounts, both self-registration accounts and access accounts, should be IP restricted to a suitable organisational IP address range and the password should be changed regularly at intervals not greater than one year. Details of shared accounts should only be issued to appropriate individuals.

Test account usage should be limited for specific purposes and passwords should be changed every two weeks.

Organisations must have audit trails for their Athens enabled accounts so that an individual can be identified by the organisation in cases of suspected abuse of Athens Terms and Conditions.

### **3. Passwords**

The selection of passwords, their use and management should adhere to best practice guidelines.

Initial passwords associated with an account should be randomly allocated and should not be deducible from the account name or any obvious formula.

Individuals should be responsible for their own password, and have a simple method of changing it.

Individuals should be advised to change the initial password and set it to something personal to them.

Individuals should be advised to follow good practices in the selection and use of passwords.

### **4. Bulk Uploads**

This section only applies to organisations that use the Athens Bulk Upload facilities.

Bulk uploads should not be used to set passwords to a fixed non-random password. Athens provides facilities to generate random passwords and structured usernames if necessary.

Bulk Upload files by their nature may contain personal data and should be treated confidentially.

### **5. Disciplinary procedures**

The organisation should have a clear disciplinary procedure for the abuse of Athens accounts.

## Username & password policy guidelines for Athens accounts

---

The organisation should have recognised contacts for Athens staff in cases of suspected abuse of Athens accounts.

Athens expects organisations to treat these requests seriously and to discuss the issues raised with the individual concerned.

All investigations and any disciplinary actions are the responsibility of the organisation itself, not Athens.

### **6. Further Information**

The UCISA Information Security Policy Toolkit provides guidance on policies and processes needed to implement an organisational Information Security Policy. It is currently only available to members of the UK academic community.

UKERNA provide useful fact sheets on Using Passwords and User Authentication. These are freely available at <http://www.ja.net/documents/factsheets.html> .

Another source of information in this area is the Internet2 InCommon Federation which has a questionnaire for US organisations who adopt Shibboleth. Its Participant Operational Practices document is available at <http://www.incommonfederation.org/docs/policies/incommonpop.html> .