St. Peter's College

Information Security Guidelines – User Management

User Management

Users should only be provided with access to services that they have been specifically authorised to use.

To comply with the University's IS Policy the College must:

1. Only provide users with access to services they require and are specifically authorized to use
2. Have a formal registration and de-registration procedure for granting and revoking access to information systems. This is achieved automatically via the core user database and via the Joiner process
3. Restrict and control allocation of system privileges
4. Review user access rights regularly, using the internal security software NETWRIX
5. Adjust access rights appropriately and in a timely manner when operational changes require it
6. Audit systems for unwanted/redundant accounts
7. Revoke access and de-register user accounts when users leave. This is achieved automatically via the core user database and via the Leaver process
8. Make all users aware of their responsibilities for information security
9. Use unique identifiers for all users' access to information systems
10. Make all users aware that user IDs should not be shared
11. Make all users aware that user passwords must never be disclosed to anyone else, unless specifically authorised by line management
12. Ensure users are advised of good security practices in the selection and use of passwords
13. Advise users on appropriate steps (such as screen locking etc) to prevent unauthorized access to machines, accounts and private information
14. Use specifically assigned IP address spaces for College visitors
15. Ensure visitors to the College are appropriately authenticated (OWL/Eduroam visitor credentials checked)

Authentication and Authorisation

There should be authentication and authorisation procedures in place to ensure users are only allowed to access services which are intended for them. Specifically for systems using techniques such as Single Sign On (SSO), controls should be in place to ensure that creating an account does not allow users access to services for which they are not authorised to use. It is also particularly important to ensure that the same password (or similar) should not be used to login to systems that are supposed to be kept secure. This applies especially to those systems that may contain sensitive personal information.

Registration and De-registration

Registration and de-registration procedures should ensure that users are assigned unique IDs so accountability can be maintained and records should be kept of all registered users. All users should sign up to a conditions of use/access agreement when they are assigned an account. There should also be means to remind users of such terms on a regular basis and ensure they are aware of any changes. Systems should be audited for unwanted/redundant accounts on a regular basis. When users leave access should be revoked and the user de-registered.

Inappropriate system privileges can be a major contributory factor in system failure and security breaches so, where possible, privileges should be kept to the minimum necessary and suitable permissions should be defined. In signing up to a conditions of use, users should be made aware of their own responsibilities.

Passwords and Unauthorised Access

Passwords should not be shared between users and it should be noted that sharing of University passwords such as SSO credentials is explicitly forbidden by the University ICT regulations. This includes giving out your password to IT support staff, IT Services or any other University department. IT Services will NEVER ask users for their passwords and so ANY correspondence (email, phone calls etc.) asking for such details should be treated with caution. Unfortunately, phishing scams are rife and users do fall for them. In order to make life simpler when users leave or are temporarily away, role based accounts and access could be considered. Where shared access to accounts is needed other means should be implemented. Project accounts, for example can be set up for clubs and societies and, within Nexus, access to email accounts can be delegated so there is no need to share passwords. If passwords need to be written down, this should be done so in as secure a manner as possible. Password management tools can be useful in order to help keep multiple passwords stored in a secure manner (KeyPass). This can be particularly useful for users who have many passwords to remember. It is important to be aware of the fact that where password exposures are known about, user accounts will be temporarily disabled. This can cause significant disruption to users who need access to critical services. It is therefore imperative that all users are made aware of their responsibilities towards password security, and of the consequences of breaching these policies. Users may also be advised to protect against unauthorised access to their own machines, accounts and private information. Obviously this will depend on the specific environment. However some examples could include simply locking office doors, password protected screen locks (e.g. where locking doors isn't possible or offices are shared), logging out of sessions on public machines, and clear desk policies.

Visitor Accounts

Visitor accounts should be specifically issued and the same University policies and practices (e.g. traceability, incident response) are applicable to visitor accounts. The University has two services available for visitors which are Eduroam-Visitor and OWL-Visitor.