Single Sign-On Terms of Use

The Single Sign-On system allows the users of services provided by PUCP units such as DTI and DCI to use only one mechanism to access those services. The services that use this system can be found at http://intranet.pucp.edu.pe/directorio-servicios.html.

The system:

1. - Allows to use a unique password for all the services, with the advantage that the user doesn't need to remember more than one password.
2. - Requires only one use of the authentication process to access many services at a time, with the advantage that the user is not prompted no enter credentials more than once (one for each service accessed).
3. - Requires only a single log out in order to close sessions for all services. This prevents users from forgetting to log off any of the services he previously accessed.
4. - Won't prevent the service from using additional signing-on mechanisms.
5. - Won't prevent the service from using additional authorization mechanisms[1].

The ***user identifier*** is a unique piece of information for each person found in PUCP database, and is used in the authentication process. The user identifier, or simply **PUCP USER**, that can be used independently of the required service, is any of the following:

- Personnel code (8 digits)
- Regular undergraduate or graduate code. (8 digits)
- Enrolled code used for a PUCP activity. For example: Prospect code, continuing education students, etc.
- Institutional email address (first part of the address without the @pucp.edu.pe or @pucp.pe domain)
- External email address used when enrolling a process/activity or when defining the "Forgot password" email address. (full address, for example. miemail@domain.com)
- For Peruvians: DNI validated by RENIEC (11 characters: 3 letters 'dni' + 8 digits of the DNI number).

For logging in using the Single Sing-on system, the user must provide username and password credentials.

This ease of access to multiple services by using a single authentication session requires that the user keeps in mind the following considerations so the experience will be safe and trustful.

1. The authentication session is only valid at the browser's windows and tabs (Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari, etc.) from which the Single Sign-On system was called.
2. When the session is ended by the "End Session" link or button from any service in use, all services sessions in the web browser will be terminated.
3. If the session is not closed by using the "End Session" links or buttons and the web browser is left opened, the user will be able to access any of the Single Sign-On services without requiring credentials input.

1 Authorization is the process in which the access to application sub-services, transactions and data is controlled.

4. If a shared computer is used, it is very important for the user to terminate the session using the “End Session” links or buttons and close the web browser (including all opened windows) completely when not using the Single Sign-On services anymore. If this is not followed, the session will remain active and the services could be accessed without requiring credentials input.
5. Only one Single Sign-On session can exist at a time for each version and Web browser type.
6. Session timeout is set to 4 hours. If the Single Sing-on system is not used during this time, all service sessions will be automatically closed, except for Campus Virtual and GMail PUCP, and authentication will be required if the user tries to access any of them. Accessing a Single Sign-On service for the first time resets the session timeout.
7. By closing a session at the Single Sign-On system, GMail PUCP and all external Gmail account sessions will be closed in the current Web browser.

PUCP is not responsible for Single Sign-On misuse consequences, such as the misuse of other people’s sessions caused by incorrect session termination.