

# xserve



respect > commitment > teamwork

**Security**  
**Roles / Abilities**  
**User Profile**

---

# Web Search Facility

---

- Web Search facility will include a feature to download search results in a csv format file.
- To support this feature it is necessary to have a defined set of parameters for users to select from when configuring their search criteria.
- The core parameters proposed to fulfil this function are:
  - Contact Reference Number (CRN)
  - Meter Point Reference Number (MPRN)
  - User Id
  - Date range
  - Contact status
- Xoserve need Shipper confirmation that these proposed parameters are acceptable



# Portal & Web Security Sign-On

---

- A common portal that allows Users single sign-on to 'Q' and IAD with potential to access other xoserve systems in the future
  - User sign on will be via the internet using URL
  - Terms of Use will be displayed at initial sign-on
  - Users need to accept Terms of Use before access granted
  - All systems will have a common look and feel
  - Users will have ID and password to sign on
  - User ID will be free format
    - User Organisations will be able to assign their own format to IDs
  - New Users will receive their account details via own email
  - Capability to manage own passwords – reset password



# Portal & Web Security Sign-On

---

- Users will be able to appoint External Administrators who will be able to:
  - Manage account portfolio for their organisation
  - Create accounts within 1 day (subject to authorisation process)
  - Amend, Suspend and Un-suspend accounts
  - Delete accounts, (Audit details /history will be maintained)
  - Reset account passwords within designated Organisation



# Security Layer

---

- A security layer sits on top of the BPMS
- It provides:-
  - Authentication & Authorisation - permissions to do / to see
  - Role allocation - e.g LSO / DLSO / User
  - Single Sign On to various applications - Q and / or IAD
  - Real time provisioning – User / Organisation / Access
  - Central system administration - access control
  - Empowered administration - delegated self service
  - Auditing of system usage – collective and individual User(s)



# Security Role Definitions

---

- System Administrator (Super User)
  - An Xoserve technical role which provides the ability to do all the security related operations across all the organisations
- Local Security Officer - aka Business Administrator / External Administrator
  - Each stakeholder organisation will have at least one or could have many who have the capacity to undertake the governance of access rights associated to the organisation group or sub division to which they are a member
- Deputy Local Security Officer – aka Delegated Business Admin
  - Appointed by the principal LSO who can do the same duties
- User
  - Holder of a Xoserve portal account for sole use for accessing applications to which they are granted permission.

# Players & Abilities

	Register User	De-register User	Application Assignment	Disable Account	Enable Account	De-Assign Application	Delegate LSO Duties	Reset Password (when locked)	Change password	Reset Password (when forgotten)	Maintain User Profile	Create & manage organisations	Register / De-register LSOs	System and technical support	Bulk set up (one time activity)
<b>System Admin</b> Xoserve	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>LSO</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						
<b>DLSO</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						
<b>User</b>									<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				

# Abilities Explained

---

- Register A User :

- The LSO / DLSO can initiate a new User account (in own organisation only) by completing mandatory and optional User profile information and submits it to security register.

- De-Register A User :

- The LSO / DLSO can terminate accounts which grant access to one or more applications. This is permanent.

- Application Assignment :

- The LSO / DLSO can grant access to Q system and/or IAD. This is the secondary part following registration.



# Abilities Explained

---

- Disable Account:
- This is the ability to suspend a Users account. The User is not able to access any web services – xoserve.com, IAD or Q system. LSO can deal with those in own organisation
- Enable Account :
- This is the re-activation of a suspended account (for same User) which restores the permissions to access services that were active prior to the disabling of the account.
- De-assign Application:
- The LSO / DLSO can withdraw User access to one or both applications (IAD and/or Q)

# Abilities Explained

---

- Delegate LSO Duties
- The expanded acronym = Local Security Officer. The principal LSO can assign the same role privileges to a nominated deputy. The DLSO can't cascade duties to anybody else. The ability to undertake security roles is contained to the organisation hierarchy that they belong to.
- Re-set Password (if locked)
- Should the User make 3 abortive attempts to guess the password, then the LSO or DLSO can reactivate it if it needs to be restored that day. A new password will be generated and sent via email to account holder

# Abilities Explained

---

- Change Password
- Typically, the User would be changing the password either when the system prompts that it requires changing or they can do it on an ad-hoc basis. The LSO / DLSO can also do this.
- Reset Password (when forgotten)
- Rather than guess the password and risk locking the account, the User can generate another password if they can input the User I.D. which match the details held in the User profile. The new password will be despatched via email to the account holder.

# Abilities Explained

---

- Maintain User Profile

- The User has the ability to maintain certain attributes held as part of their profile held in the security register. Example : Name, Telephone No., email address.

- Create and Manage Organisations

- This ability is limited to Xoserve to set up and maintain organisation hierarchy for all stakeholders who are needing to interact with our services.

- Register / De-Register LSOs

- In order for organisations to be self sufficient for managing the portfolio of Q and IAD accounts they need to appoint LSOs. Over time the registration / deregistration will continue – *process to be firmed up.*

# Abilities Explained

---

- System & Technical Support
- Restricted to Xoserve System Administrators who have abilities to maintain and support the software and influence security policies and rules.
  
- Bulk Set Up of accounts (one time only)
- Prior to inception of the new Q system, Xoserve can bulk create User accounts for each stakeholder organisation subject to submitting a csv file completed with mandatory User profile information.