Trusted Information Sharing Network
for Critical Infrastructure Protection

USER-ACCESS MANAGEMENT—OVERVIEW FOR CEOS

All organisations need to control access to both information and information systems and this can be achieved by managing user access. This is particularly relevant for critical infrastructure organisations as the information they hold can be highly sensitive and of significant importance to the safety and well being of the community.

User-access management has two simple objectives:

- ensuring only authorised users have access, when needed
- preventing unauthorised access to information and systems.

Achieving these objectives requires organisational knowledge of:

- information assets—what you are trying to protect and its importance for the organisation's ongoing business functions
- users—who the authorised users are, both within and outside the organisation
- privileges—which users require access to which information assets, to what extent, and in what circumstances.

A defence in depth strategy emphasises the need for organisations to examine their IT and operating environments to identify weak points—whether people, processes, technology or governance—and similarly to implement controls across all these areas.

Complementing the core principles of defence in depth and the overarching principles of information security, user-access management itself has a series of core guiding principles, as follows:

1. **'Least privilege'—**providing the least amount of access necessary for a given user to complete their business role.
2. **'Need to know'—**providing access to systems and information only where there is a need for the recipient of such access to have it
3. **'Controlled access'—**defining procedures to monitor, enable and disable access, and enforce security policy at all access points

Effectively applying these principles to organisational processes, technology and personnel ensures that user-access related risks are appropriately managed, ensuring authorised access is available when required and unauthorised access is prevented.

Issues to raise with your CIO

The following is a suggested list of issues to discuss with your CIO in reviewing the organisation's user-access management.

Governance
• Do you understand all avenues for system and information access? • Have enterprise data, processes and job functions been clearly categorised and their security needs identified? • Is there an existing user-access management policy?   - Is this policy practically enforced through documented procedures?
People
• Is separation of duties and job rotation implemented? • Are external parties appropriately vetted before being granted system access? • Are users aware of their obligations to protect organisational information?
Operations
• Is a formal and documented process used to authorise and create accounts when personnel join the organisation? • Is user access regularly audited, changed along with role changes and removed at the point of employee termination?
Technology
• Do access controls correspond to business objectives, operational practices, and security categories of associated data sources? • Are network, application, host and information-level access controls used cohesively to provide a layered set of defence in depth controls?

Clearly categorising the security requirements and status of all information and enterprise processes, as well as clearly defining security roles and responsibilities is required. Every organisation is different and should therefore review their risk management plan to ensure their organisation is appropriately protected.

This information has been developed by the IT Security Expert Advisory Group which is part of the Trusted Information Sharing Network (TISN) for critical infrastructure protection. More information on TISN can be sought from www.tisn.gov.au or by contacting cip@ag.gov.au.