Controlling Access to Information Systems Policy Statements

User

Mobile phones, tablets, portable computers, laptops, USB devices or any other device must not be connected to DCC's internal computer systems or networks unless the device has been approved for use by the IT Manager.

Users should not access systems that contain personally identifiable information (PII) from mobile devices or save any PII information onto USB devices etc unless approval has been given by the IT Manager.

Manager

Managers must promptly report all significant changes in user duties or employment status to IT Helpdesk staff who are responsible for managing user accounts and the allocation of system privileges.

Written approval is required from a Department Manager authorised to delegate user privileges before the IT Helpdesk can add new users to the systems and grant access privileges. The access requirements for the new user must be provided by the Department Manager and this is achieved by completing the appropriate form and forwarding it to the IT Helpdesk.

System privileges granted to general users must be re-evaluated by Department Managers every twelve (12) months. Special Access privileges must be reviewed every six months and signed off by the Chief Information Officer. This re-evaluation involves assessing whether the current level of system privileges are still required to perform the user's job duties. Any anomalies should be referred immediately to the Chief Information Officer.

Technical

DCC mandates the use of access controls and other security measures to protect the confidentiality, integrity and availability of its information and systems. No responsibility will be accepted for the loss of personal data or software that may occur during routine system administration functions - e.g. identifying and removing any software or file that is non-work related.

Access privileges must be associated with an individual user ID which uniquely identifies only one user. Shared, Generic or Group User IDs are not permitted unless specifically authorised by the Chief Information Officer who will keep a record of the exceptions. System to system connections must also be uniquely authenticated.

Users must only be allocated one User ID to gain access to information systems resources owned or managed by the Council and this user ID must conform to the naming standards specified by the Chief Information Officer - e.g. login name jackiek. The only exception to this requirement is where staff require special, higher level privileges for the purposes of system, application or network management and they are provided with an additional User ID for these duties. Where special privileges are needed, ordinary work should be carried out using the normal user ID and application, system or network administration carried out with the User ID granted for this purpose.

Once a user leaves DCC the user's ID must not be reallocated to another user.

Information which is sensitive, critical, classified or unclassified but valuable must be protected by contractual, physical and system access controls so that it is not inappropriately disclosed, modified or deleted.

After logging in to a system or application, users must be kept within the system or application menus which restrict them to the access options that they have been authorised to use. Command prompt functionality should only be available to those that require it for the purposes of system or application management.

The IT Helpdesk must maintain up to date records for all user IDs including the networks, systems and applications that each user has been granted access to. This information will enable privileges to be changed or removed at short notice.

An approved software licence management application should be used to ensure that DCC does not exceed the number of licenses purchased and to detect and prevent unauthorised software from being run on networks and computers.