

**SUBJECT:** Enterprise Administrator Access

**PURPOSE:**

Employment Security Department (ESD) Information Technology (IT) resources must be secured and maintained. Primary responsibility for maintenance is designated to specific staff. However, there may be times when Information Technology Services Division (ITSD) staff must perform emergency maintenance. For this reason, administrator account access to all ESD Network Attached Devices is to be set up and communicated to Key Production Control Security Staff in accordance with this policy.

**DEFINITIONS:**

Network Attached Devices: Network Attached Devices include, but are not limited to: servers, routers, switches, firewall, VPN concentrators, wireless access points, desktops/PCs, intrusion detection devices, and printers.

Key Production Control Security Staff: These staff are the lead ITSD Security Analyst and the Production Control Manager.

Security Service Account: An administrative account used by Key Production Control Security Staff to gain or allow emergency access to Network Attached Devices when a technical emergency has been declared.

Device Manager: Anyone who is responsible for password control of network-attached devices not supported by Security Service Accounts.

Technical Emergency: A technical emergency is declared when there is a serious threat or risk to ESD's technology infrastructure or its application environments. The criterion is the existence of a technical problem or threat to agency systems that significantly impedes the ability to do business and serve the needs of ESD customers.

**POLICY:**

All ESD owned and maintained Network Attached Devices are to have a Security Service Account established for emergency use whenever it is technically and operationally feasible. When use of a Security Service Account is not feasible, the Device Manager will provide a password to Key Production Control Security Staff for administrator access to the device. The passwords for these accounts are to be changed at the start of each month using the password change process outlined in this policy. Upon changing the password, the Device Manager is to notify Key Production Control Security Staff of the change. Devices under a support contract or agreement are to be noted as to the limits of what actions may be performed on them.

The account information is to be retained in a secured mainframe dataset and on printed copies stored in safes at both the Lacey 605 Woodland Square Loop building and the Olympia 212 Maple Park building.

In the event of a technical emergency, the Security Service Account information may be disseminated to key individuals as directed by an ITSD Deputy Assistant Commissioner or higher. These key individuals will be assigned to perform specific actions in an effort to restore, or prevent the loss of, service. Any actions taken on devices under support contracts or agreements must be consistent with, and not exceed, what is noted in the agreement to avoid nullifying them.. Upon the use of the enterprise administrator access, the Device Manager is to be notified, and the account password changed at the earliest opportunity.

The relationships between Network Attached Devices are such that if one fails or is compromised, it often impacts other devices. For this reason, devices not in compliance with this policy may be disconnected from the network.

### **Password Change Process**

Passwords for the administrator access are to be changed at the beginning of each month as follows:

1. Key Production Control Security Staff will change the password on all Security Service Accounts for which they have responsibility, by the first working day of each month.
2. The Device Manager will change devices that require manual intervention to change the password, by the first working day of each month.
3. The Device Manager verbally informs Key Production Control Security Staff that the new password is in place. Passwords are never to be revealed in writing, through e-mail, or by voice mail. If Key Production Control Security Staff are unavailable, a message is to be left for them that a new password has been created.
4. Key Production Control Security Staff will place the device, account and password information in a secured mainframe dataset accessible to them through a specially created mainframe account.
5. Current printed copies listing the device, account and password information will be placed in two safes: one copy in a safe at the 605 Woodland Square Loop building in Lacey and one copy in a safe at the 212 Maple Park building, by the second Monday of each month.

Note: The password is disclosed only after a technical emergency has been declared, and then only if needed to access specific devices to resolve the emergency condition.

**Emergency Use of Enterprise Administrator Access**

Use of enterprise administrator access is to occur only when a technical emergency has been declared and an individual has been authorized for access by a manager at the ITSD Deputy Assistant Commissioner level or higher. The following steps are to be used for obtaining account and password information:

1. The ITSD Deputy Assistant Commissioner who authorized use of the enterprise administrator access contacts Key Production Control Security Staff and notifies them who has been authorized and how the authorized person can be reached.
2. The Key Production Control Security Staff will contact the authorized individuals with the account and password information.
3. Following the technical emergency, Key Production Control Security Staff will notify the Device Manager that the enterprise administrator access information was disclosed and the password must now be changed.
4. The Key Production Control Security Staff and /or the Device Manager will follow the password change process outlined in this policy.

If Key Production Control Security Staff cannot be reached, or timeliness is a concern, either of the following alternatives can be used in place of steps 1 and 2 above:

**Alternative 1 - Use of special mainframe account**

A mainframe account has been established for the sole purpose of accessing the enterprise administrator access information.

1. The ITSD Deputy Assistant Commissioner may provide the mainframe account and password to the individual being authorized.
2. Using the most convenient means available for accessing the mainframe (i.e., OC WebConnect, Attachmate Extra, Host On Demand, or dumb terminal), the authorized individual will log on to a mainframe TSO session.
3. The authorized individual will be able to view a screen containing the enterprise administrator accounts and Security Service Account passwords.

**Alternative 2 - Access to safe**

If access to the mainframe is also impaired, the authorized individual may be given access to the Production Control safes.

1. The ITSD Deputy Assistant Commissioner who authorizes use of the enterprise administrator access provides the safe combination to the authorized individual.
2. The authorized individual unlocks the most easily accessible Production Control safe, obtains the information needed from the printed version of the enterprise administrator access list, and places the list back in the safe.

**FOR FURTHER INFORMATION:**

Contact the ITSD Production Control Manager or the IT Architecture Deputy Assistant Commissioner via the agency's e-mail system.