Title: Encryption Key Management Procedure
Reference Number: 6.3.2.1

Purpose
This procedure provides guidance on how encryption keys are managed.

Obtaining SSL Certificates

Entrust Contract, Standard SSL Certificates

- A Certificate Signing Request (CSR) is generated from an authorized System Administrator. The Organization MUST BE "Old Dominion University".
- This CSR is stored in the directory /incidents/Certificates on server Guadalcanal. The filename should be %HOSTNAME%%DATE%.csr
- The CSR is given to Entrust via the Certificate Administrator. Located at certadmin.entrust.com username=7576834580 pass=<REMOVED>
- Entrust produces a Certificate from the CSR. It is a text block that must be copied/pasted into documents.
- A Copy of the text block is stored in directory /incidents/Certificates on server Guadalcanal. The filename should be %HOSTNAME%%DATE%.crt

Non Contract, Standard SSL Certificates

- A Certificate Signing Request (CSR) is generated from an authorized System Administrator. The Organization MUST BE "Old Dominion University".
- This CSR is stored in the directory /incidents/Certificates on server Guadalcanal. The filename should be %HOSTNAME%%DATE%.csr
- The Security Administrator will work with the System Administrator during the purchase.
- If a renewal password/passphrase is required. It will be set by the Security Administrator. These passwords/passphrases are currently located in directory /incidents/Docs/SSL-Keys-Info/Entrust-Non-Contract-Passphrase on server Guadalcanal. Those that are not the standard are saved in the same directory and will be migrated to the standard at the next renewal.
  - The Technical contact is the Current Security Administrator.
  - The Authorizing contact is the Current ISO.
  - The Budget/Billing Contact is current OCCS Business Office Manager (Earl Gower).
  - The business address is what is currently listed in the university phonebook.
  - The Certificate Company Generates the Certificate.
- A Copy of the text block is stored in the directory /incidents/Certificates on server Guadalcanal. The filename should be %HOSTNAME%%DATE%.crt

Non-Contract Standard SSL Certificates should be moved under the contract when possible.

Non Standard, Non Contract, SSL Certificates

These are for non-webserver certificates. Usually used in mail/custom applications. This is an all encompassing procedure that should be used as a guide at best. It is a catch all and should be treated as such. An example would be the FSA-Atlas certificate. It is not a standard web certificate and when it comes time for renewal, should follow this procedure.

- If a certificate request is generated it should be stored in the directory /incidents/Certificates on server Guadalcanal.
If a renewal password/passphrase is required. It will be set by the Security Administrator. It should use the directory /incidents/Docs/SSL-Keys-Info/Entrust-Non-Contract-Passphrase on server Guadalcanal when possible.

- If a Technical Contact is required, the current Security Administrator should be used.
- If an Authorizing contact is required, the current ISO should be used.
- If a Budget/Billing Contact is required, the current OCCS Business Office Manager (Earl Gower) should be used.
- The business address is what is currently listed in the university phonebook.
- The Certificate Company Generates the Certificate.
- A Copy of the text block is stored in the directory /incidents/Certificates on server Guadalcanal. The filename should be %HOSTNAME%-%DATE%.crt

## Distribution of Encryption Keys

- The Security Administrator copies the encryption certificate text block onto a USB drive used for key distribution.
- The Systems Administrator ‘checks out’ the encryption key USB drive from the Security Administrator. The encryption key USB drive should not be ‘checked out’ over night. It should be returned immediately after use, usually within one hour of check out.
- The Systems Administrator installs the encryption certificate from the encryption key USB drive onto the system to be secured.
- The System Administrator returns the encryption key USB drive to the Security Administrator and the key is ‘checked’ back in.
- The Security Administrator cleans the USB key of all data and prepares it for next use.

## Storage and Backup of Encryption Keys

- The OCCS Safe is opened by a member of the OCCS Operations staff who knows the combination to the safe.
- The Systems Administrator unlocks the ‘Encryption Key’ lockbox with a key that is only retained by the OCCS Security staff. Note: The OCCS Security Staff do NOT know the combination to the OCCS safe.
- The Systems Administrator retrieves the two USB memory sticks from the lockbox.
- Both the Operator and the Security Administrator fill out the Encryption Key Log that is in the binder.
- The Security Administrator is responsible for re-locking the lockbox.
- The Operations staff is responsible for locking the safe.
- The encryption key text block is then is written to two USB memory sticks from the security server Guadalcanal by an authorized OCCS Security Administrator.
- The encryption key text block is printed to paper and dated by an authorized OCCS Security Administrator.
- The OCCS Safe is opened by a member of the OCCS Operations staff who knows the combination to the safe.
- The Systems Administrator unlocks the ‘Encryption Key’ lockbox with a key that is only retained by the OCCS Security staff. Note: The OCCS Security Staff do NOT know the combination to the OCCS safe.
- The Security Administrator places the USB memory sticks and the printed encryption key block in a binder that is stored in the encryption key lockbox.
- Both the Operator and the Security Administrator fill out the Encryption Key Log that is in the binder.
- The Security Administrator is responsible for re-locking the lockbox.
- The Operations staff is responsible for locking the safe.
Revoking Encryption Keys

- The Security Administrator is informed of the need to revoke an encryption key through an investigation, request to renew a certificate, a problem ticket or direct communication with a Systems Administrator.
- The Security Administrator will access the secured web site of the issuing authority and use the established process of that site to revoke the encryption key certificates.
- The Security Administrator will inform the appropriate Systems Administrators that the certificates have been revoked.
- If new certificates are to be issued, then the new encryption key process is followed.
## Encryption Key Log

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Operator</th>
<th>Sec Admin</th>
<th>Purpose</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Old Dominion University  
Technology Policies, Standards, Procedures and Guidelines

Definitions

**Information Technology Resources** are defined as computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services.

**OCCS** is the acronym for the official name of the Office of Computing and Communications Services.

**User** includes anyone who accesses and uses the Old Dominion University information technology resources.

---

### Policy References

ODU faculty, staff and students are bound by all applicable laws, policies, standards and procedures and guidelines. For reference, some frequently referenced documents are noted. This is a non-inclusive list and not intended to limit applicability of any other law or policy.

| Policy Foundation: | Federal and State Law  
|                   | Policy 3505 Security Policy  
|                   | COV ITRM standard SEC501-01 |
| Related Standards: |  |
| Related Procedures, Forms: | Encryption Key Log |
| Related Guidelines: | None |
| Maintenance: | Office of Computing and Communications Services |
| Effective Date: | Reviewed on an annual basis |

- Approved by: Pending: Rusty Waterfield  
  Acting Assistant Vice President, Office of Computing and Communications Services

- Approved: Pending: University Advisory Council on Technology

  - Required for Standard