# Security Management and Consulting

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Security Management and Consulting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This service supports the University's security policies and processes by providing appropriate controls over access to service infrastructure components and protecting services from unauthorized access or use. This service also provides consulting services to ensure departments and systems comply with the University's security requirements.</td>
</tr>
<tr>
<td>Eligibility</td>
<td>All University Departments</td>
</tr>
<tr>
<td>How to Request Service</td>
<td>IT Service Request</td>
</tr>
<tr>
<td>Availability</td>
<td>Business Standard - Service availability target is Monday- Friday 8:30 am. – 5:00 p.m. No on-call engineer support provided. Support Service is Next Business Day. Full Support Center Service request schedule is available.</td>
</tr>
<tr>
<td>Charges</td>
<td>Use of external security resources may incur charges</td>
</tr>
<tr>
<td>Service Line</td>
<td>Systems and Networks</td>
</tr>
</tbody>
</table>

### Features
- Establishes monitoring and reporting processes for security events and ensures that all recognized events are logged, and reported on.
- Plans and designs hardware and software solutions used to support security processes and automated enforcement of University security policies.
- Establishes guidelines for appropriate access control lists, group membership, rights assignments and access profiles.
- Consults and recommends physical security solutions such as badge creation and maintenance, camera surveillance, physical access management to secure areas and biometric or other multi-factor access methods.
- Establishes appropriate protocol management services such as encryption support, VPN access and secured transmission of data and files.
- Negotiates and establishes appropriate presence management services such as federated identity management and trusted partner support.
- Plans and allocates resources to support internet firewalls, network port access and proxies.
- Consults with University departments on security requirements for application security, security models, application security API interfaces and security validation.
- Negotiates with 3rd party firms to conduct regular audits and tests for intrusions, vulnerability and security risk exposures.
- Support external audit efforts as well as validate security compliance with regulatory and industry controls.
- Provide security consulting services to assist with security design over new and changing services.
- Reviews IT practices for compliance with University Information Security interests.
- Works with Technology Training service to ensure appropriate campus community training on information security roles and responsibilities.

Owner | Dexter Caldwell |
--- | --- |
Pre-requisites | Adequate power and networking environment for security infrastructure. |
VP Customer | Vice President of Finance & Administration |
Delivery Channels | Complete Work Requests, Security plans and strategies, Consulting and Support |
Service Targets | Major Server Vulnerability Rate. (Quarterly Major Server Vulnerabilities/Total Servers Scanned.)
| Total Server Vulnerability Rate. (Total servers with vulnerabilities/Total Servers Scanned.)
| Staff Security Training Rate. (University Faculty/Staff with PII access trained/Total Faculty and Staff.)
| PCI Compliance Rate. (PCI compliant Apps/Total Apps requiring PCI compliance.)