## Incident Response

### Service Name
Incident Response

### Description
This service implements the University’s security policies and processes as directed by Security Management. This service responds to security incidents and malfunctions, and ensures the University follows an incident response program with appropriate reporting, discovery, investigation, recovery, and follow-up for information security incidents.

### Eligibility

#### How to Request Service
- Approved work Requests
- Escalated Incidents or Problems from the IT Service Center
- approved operational run procedures
- Security incidents, alarms and alerts

### Availability
Business Preferred - Availability target is 24X7X365 except for scheduled maintenance, holidays or dependent party outages. Systems may have limited or no redundancy. Systems have receive priority support during business hours. Limited on-call support response may be available outside of business hours. Full Support Center Service request schedule is available.

### Charges

<table>
<thead>
<tr>
<th>Service Line</th>
<th>Systems and Networks</th>
</tr>
</thead>
</table>
| Features              | Provide monitoring and reporting on security event ensuring all recognized events are logged, escalated and reported on.  
                        | Investigate and report on security breaches.  
                        | Provide management and maintenance of certificates.  
                        | Build, test, implement and customize hardware, software and directories used to support security solutions and automated enforcement of University security policies.  
                        | Build, manage and maintain access control lists, grouping assignments, rights assignments and access profiles.  
                        | Provide and maintain protection over viruses and intrusion threats.  
                        | Build, manage and maintain physical security solutions such as badge creation and maintenance, camera surveillance, physical access management to secure areas and physical authentication such as thumb or retina biometrics access.  
                        | Provide protocol management services such as encryption support, VPN access and secured transmission of data and files.  
                        | Provide presence management services such as federated security management and trusted partner support.  
                        | Design, build, implement, test and maintain internet firewalls, internet port access and proxies.  
                        | Recommends standards for application security, security models, and security validation.  
                        | Work with 3rd party vendors for routine audits and tests for intrusions, vulnerability and security risk exposures.  
                        | Recommend and implement measures to address security risk exposures.  
                        | Provide security patch management services.  
                        | Provide security consulting services to assist with security design over new and changing services.  

### Owner
Wayne Craig

### Pre-requisites
Adequate power and operating environment.

### VP Customer
Vice President of Finance and Administration

### Delivery Channels
- Complete Work Requests
- Security audit reports
- Network and security systems monitoring

### Service Targets
- Incident Resolution Rate. (Incidents resolved within agreed service level/Number of incident occurrences.)
- Community Incident Impact Rate. (Number of incidents with community input/total incidents.)
- 95% of incidents resolved within 3 business days