**ADM 419**

**Appendix F – Security Incident Response Log**

|  |  |
| --- | --- |
| **Incident Identification Information** |  |
| Name: |  |
| Phone: |  |
| Email: |  |
| Date/Time Detected: |  |
| System / Application Affected: |  |
| **Incident Summary** |  |
| Type of Incident Detected:  (Denial of Service, Malicious Code, Unauthorized Access, Unauthorized Use / Disclosure, Unplanned System Downtime, Other ) |  |
| Description of Incident: |  |
| Names of Others Involved: |  |
| **Incident Notification** |  |
| How Was This Notified?  (Security Office, IT Personnel, Human Resources, Other) |  |
| **Response Actions**  **Include Start and Stop times** |  |
| Identification Measures (Incident Verified, Accessed, Options Evaluated): |  |
| Containment Measures: |  |
| Evidence Collected (Systems Logs, etc.): |  |