UGA Computer Equipment, Software, or Services (CESS)

Security Evaluation Form

Instructions: Fill out all applicable parts 1-4 of this form, save, and then submit to the Office of Information Security for review by attaching the completed form in .pdf format to the related CESS Approval in UGAMart at https://ugamart.uga.edu. Please direct any questions or comments on this form to the Office of Information Security via the EITS Helpdesk at 706-542-3106 or helpdesk@uga.edu.

Part 1 - Responsibility for Security.

1.1 Please indicate who will be responsible for the security of this resource:

Name:

Title:

Department/College:

1.2 Is the individual responsible for the security of the resource aware that the University of Georgia has policies and guidelines regarding the privacy and security of systems and information--including the Privacy Policy, Password Policy, Minimum Security Policy, Guidelines for Handling Sensitive Data, and Guidelines for Trusted Computing--and that these policies and guidelines can be found at https://infosec.uga.edu/policies?

☐ Yes

☐ No

Part 2 - Sensitive Information. If the resource will process, store, or transmit Sensitive Information as defined in the University's Information Classification Standard, complete Part 2 to describe the Sensitive Information and the security plan for protecting it. Otherwise, skip to Part 3 and leave the questions in Part 2 blank.

2.1 What type of sensitive information? (check all that apply)

- [ ] Social Security Numbers
- [ ] Financial Account Numbers and Information (GLBA)
- [ ] Credit Card Numbers or Transactions (PCI DSS)
- [ ] Patient Health Information (HIPAA)
- [ ] Student Records (FERPA)
- [ ] Human Subjects Research
- [ ] Other :

2.2 How will the resource handle the sensitive information? (check all that apply)

- [ ] Stores sensitive information
- [ ] Processes sensitive information
- [ ] Transmits sensitive information

2.3 How much sensitive information will the resource potentially store? If the resource will not store sensitive information, how much will it process or transmit annually? (check one)

- [ ] 0 - 1,000 records
- [ ] 1,000 -10,000 records
- [ ] 10,000 - 50,000 records
- [ ] 50,000 – 100,000 records
- [ ] 100,000+ records

2.4 Briefly describe the security plan for this CESS resource. Include the various administrative, technical, and physical safeguards that comprise the security plan. The following are examples of common safeguards.

Administrative: departmental security policies and standards, background checks, procedures for updating accounts and access, procedures for secure disposal/surplus, separation of duties, risk assessments, compliance efforts, etc.

Technical: firewalls, limited network access/ports, routine vulnerability scanning, patch management, change management, encryption, logging and monitoring, etc.

Physical: lockable doors and windows, security cameras, card swipe access, environmental controls, security cables and locks, etc.

Part 3 - Critical Systems. If the resource can be classified as a Critical System as defined in the University's Information Classification Standard, complete Part 3 to describe the critical nature of the resource and any contingency plans that exist. Otherwise, skip to Part 4 and leave the questions in Part 3 blank.

3.1 Impact. What are the categories of impact to the University if resource became unavailable. (check all that apply)

- ☐ Risk to Life: loss of availability will create increased risk to life or otherwise create risk to individuals (e.g. health care information or emergency notification system)
- ☐ Mission Risk: loss of availability or downtime would preclude the University of Georgia from accomplishing any of its core functions or its mission.
- ☐ Compliance Risk: availability is mandated by law or required by contract.
- ☐ Reputation Risk: loss of availability will cause significant damage to University reputation.
- ☐ Financial Risk: loss of availability will cause the University to incur significant costs or lost revenues.
- ☐ Other:

3.2 Maximum Tolerable Downtime. How much time could the resource be unavailable before impacting the University? (check one)

- ☐ < 1 day
- ☐ Days
- ☐ Weeks
- ☐ Months

3.3 Recovery Time Objective. What is the approximate desired timeframe for recovering the resource if it were to become unavailable? (check one)

- ☐ 1 hour
- ☐ 1 day
- ☐ 1 week
- ☐ 30 days
- ☐ over 30 days

3.4 Briefly describe the contingency plan or disaster recovery plan that will be used to recover the resource if it becomes temporarily unavailable. Be sure to include preventative safeguards (e.g. uninterruptible power supplies, backup generators, fire suppression, backups of data, redundant systems, etc.), recovery strategies (e.g. recover from backup, recover from an alternate site, equipment replacement, etc.), and strategies for testing the plan (e.g. tabletop exercises, functional exercises, simulations, etc.). For security purposes, do not include any specific information regarding names or locations of any recovery facilities or systems.

Part 4 - Internet Access. If the CESS resource will be connected to the Internet, please complete Part 4. Otherwise, leave the questions in Part 4 blank.

4.1 Briefly describe any measures that will be taken to protect the resource from the Internet-based attacks or intrusions. If you have already listed these measures in your answer to Part 2.4, please indicate below.

Completed By

Name:

Title:

Department/College:

Date: