GA•AWARDS External Research Request Security Review Rubric

Application Number: _____ Application Name: _____ Date Received: _____			
Reviewer Name: _____ Review Date: _____			
Exemption For ISO 27001 Certification.	◯ *Data environment is certified ISO 27001*		
Criteria	**Exemplary**	**Satisfactory**	**Unsatisfactory**
Physical Access Controls	Limited access to data storage facility. All entrances are keyed and only individuals who have signed the Confidentiality and Data Usage Agreement have access. All entrances are covered by surveillance and all access is logged and there are routine audits of access logs to ensure compliance. Trusted user list is routinely audited for currency.	Limited access to data storage facility. All entrances are keyed and only individuals who have signed the Confidentiality and Data Usage Agreement have access. There are minimal concerns regarding entrance surveillance, access logs, **OR** auditing of access logs. Trusted user list is routinely audited for currency.	There are significant concerns regarding access to data storage facility **OR** monitoring of the data storage facility **OR** access logs **OR** auditing of access log or trusted user list.
Logical Access Controls	Two-factor authentication is enabled. Strong passwords required; minimum length of 16 characters or greater. Password expiry is forced quarterly or more frequently.	Single or two-factor authentication. Strong passwords required; minimum length of 16 characters or greater. Password expiry is forced every six months or more frequently.	Single factor authentication. Weak passwords: outdated complexity requirements or minimum length of less than 16 characters. Password expiry is not forced or forced at intervals greater than six months.
Encryption	Data is secured using the strongest allowable FIPS 140-2 encryption: AES 256 for data at rest. TLS or SSL v3 for data in transit or IPSEC VPN.	Data is secured with the FIPS 140-2 minimum strength encryption: AES 128. SSL and TLS v3 for data in transit or IPSEC VPN.	Encryption of data is not present or does not meet FIPS 140-2 standard.
Network Security	Secure Server located on segmented network with: Advanced firewall, Network Intrusion Detection, Verbose logging with quarterly or more frequent audits, IPSEC or TLS VPN for external access to network. Access to network limited to individuals who have signed the Confidentiality and Data Usage Agreement **OR** Physically isolated network with no exterior access.	Secure server located on segmented network with: Firewall, logging and quarterly audits, IPSEC of TLS VPN for external access to network. Access to network limited to individuals who have signed the Confidentiality and Data Usage Agreement **OR** Physically isolated network with no exterior access.	Server is located on shared network with individuals who have not signed the Confidentiality and Data Usage Agreement **OR** Firewall is not present or not logged and audited **OR** Any data is passed over the network in plain text.

GA•AWARDS External Research Request Security Review Rubric

Workstation Security	Workstation has current anti-virus, anti-malware. Strong logical controls for authentication to individuals who have not signed the Confidentiality and Data Usage Agreement. Workstation is in physically secured location. Data are encrypted when stored on workstation. Network is encrypted when connected to secured server. **OR** Workstation is stand-alone with no network connection and has other aforementioned controls	Workstation has current anti-virus, anti-malware. Strong logical controls for authentication to individuals who have not signed the Confidentiality and Data Usage Agreement. Data are encrypted when stored on workstation. Network is encrypted when connected to secured server **OR** Workstation is stand-alone with no network connection and has other aforementioned controls	Multi-user workstation **OR** workstation with weak or no access controls **OR** Data are not encrypted on workstation **OR** connection to secure server is not encrypted **OR** there is no anti-virus **OR** there is no anti-malware.
Data Destruction Plan	Plan demonstrates efficacy of data disposal methodology in compliance with Confidentiality and Data Usage Agreement. The exact methods of data destruction are submitted for review with application, which includes the specific type of storage media on which data will be stored and the media type and destruction method of any backups. Destruction method includes the name of all software used and the settings of said software with regard to the rigor of destruction.	Plan demonstrates efficacy of data disposal methodology in compliance with Confidentiality and Data Usage Agreement. Methods are described in sufficient detail but lack some of the exact specifications. Discussion of different types of storage media including backup media are included in existing or proposed method of data destruction.	Plan does not sufficiently address efficacy of data disposal methodology or data storage media are not known or are not addressed.
This rubric is used by GOSA to assess the security of external researcher's data storage facility.			