

Attachment D

NPERS INFORMATION SECURITY REQUIREMENTS

The Nebraska Public Employees Retirement Systems (NPERS) has established a comprehensive information security program to protect the confidentiality, integrity, and availability of retirement plan member information as well as any other information owned, controlled, or managed by NPERS. NPERS requires all Business Partners, Contractors, and Subcontractors (hereinafter "Contractor") to materially comply with this Information Security Attachment to satisfy the minimum requirements of NPERS's information security program. All Contractors who wish to conduct business with NPERS shall agree to implement robust security measures designed to:

- Ensure the security and confidentiality of NPERS Data;
- Protect against any foreseeable threats or hazards to the security or integrity of NPERS Data;
- Protect against unauthorized access to or use of NPERS Data and Contractor's systems;

As part of this Request for Proposal, please review all the following requirements, and indicate your willingness to comply with these requirements or provide reasons that you will not be able to comply.

1. GENERAL REQUIREMENTS

In all cases, NPERS requires that:

- All system security incidents involving this relationship or NPERS information shall be reported to NPERS's Information Technology Manager (or designate) at the earliest possible time at jack.hardy@nebraska.gov and by phone at (402) 471-7076. This notification must occur NO LATER THAN 2 hours of Contractor becoming aware of an actual or potential incident, even if the incident is not confirmed. Notification must include enough detail so that NPERS can assess the scope and impact of such potential incidents and take additional action as necessary to safeguard the information and/or report to authorities.
- Contractor shall brief all Contractor personnel, including employees and contractors with access to the NPERS Data, on the confidentiality and protection of NPERS Data (which shall include secure coding practices, if applicable). All Contractor personnel are prohibited from accessing any NPERS data until they have been briefed on security requirements of NPERS.
- Contractor shall perform a criminal background check on all personnel with access to NPERS information. Contractor will not allow any personnel with a criminal background access to NPERS information unless approved by the NPERS IT Manager.
- Access to NPERS Data for Contractor Personnel shall be on a "need-to-know" basis and restricted to allow only the minimum information required to fulfill contract requirements. Contractor shall provide a list of all Contractor personnel with access to NPERS data when requested by NPERS.
- Access privileges to Contractor Personnel shall be assigned to individually identifiable accounts, and all activity conducted by these accounts must be auditable. Such access privileges shall be managed through the use of user ID's and passwords and shall not be shared or migrated to another individual. Additionally, biometrics, key tokens, or other security features that uniquely identify individuals may be used and are recommended. Auditable Events for Access Control include, at a minimum, successful logon and logoff to domains with access to NPERS data, physical entry to secure areas, failed logon attempts, and all privilege account (such as System Administrator) activity related to the NPERS data and systems. Contractor will provide NPERS with a list of Access Control auditable events and evidence of logging and monitoring these auditable events related to NPERS when requested by NPERS.
- Contractor shall take commercially reasonable steps to prevent additional harm caused by security incidents and prevention of damage from an incident shall always take priority over forensics. This means that if Contractor discovers an incident in process, the priority shall be to prevent any damage over collection of any evidence. Contractor is required to provide NPERS with a formal root cause analysis for all security incidents within 2 weeks of any security incident.

- Contractor's protection of NPERS Data shall be consistent with the terms of the agreements (the "Contract Documents") between NPERS and Contractor and all applicable laws and regulations, including Industry Standard Safeguards as described in ISO-27001/27002.
- Contractor shall designate an individual who shall serve as NPERS's ongoing single point of contact for purposes of addressing issues with respect to the use and security of NPERS Data during the term and following the termination or expiration of the Contract Documents. Such individual will be accessible to NPERS 24 hours per day, and will cooperate with NPERS to address such issues. If this individual is expected to be unavailable for more than 1 day, or if the Contractor removes this individual from this responsibility, Contractor shall notify NPERS's IT Manager immediately.
- Contractor shall not outsource any of its security program affecting NPERS unless approved in advance by the NPERS IT Manager.

2. SECURITY MEASURES

- Contractor shall maintain a written comprehensive information security program that is documented in a "System Security Plan for NPERS", and shall provide documentation of their security policies, standards, and procedures to NPERS's IT Manager upon request. The System Security Plan shall be a formal and highly secured document which describes the controls, processes, architecture, and protocols used to protect NPERS information. Access to this System Security Plan shall be restricted to personnel with an approved business need for this information.
- Before contract effective date and annually thereafter, Contractor will provide NPERS with a copy of the System Security Plan which details the Contractor's security program around NPERS data confidentiality, integrity, and availability. Contractor's System Security Plan should be provided to NPERS as part of the RFP. NPERS will treat this plan as a Highly Confidential document with commensurate security.
- Contractor shall establish and maintain safeguards against the destruction, loss, alteration or misuse of NPERS Data in the possession of Contractor using safeguards that are no less rigorous than those used by Contractor for its own information of a similar nature. These safeguards will be described in the System Security Plan.
- Contractor shall remediate security findings or risks in a manner acceptable to NPERS's IT Manager. Upon request, Contractor shall provide security corrective action reports and remediation progress to NPERS and allow access as necessary to inspect progress of such remediation. If such findings or risks cannot be remedied or mitigated in a mutually agreeable manner, NPERS may terminate this agreement and request the return or destruction of all NPERS data.
- Contractor shall communicate and coordinate any changes to Contractor's security infrastructure which directly affect the security of NPERS Data. Contractor shall not modify any part of the security posture of NPERS unless this is coordinated in advance with the NPERS IT Manager. This includes any changes to the hardware, software, or any technical services that may indirectly have an impact to the Contractor security posture.
- If Contractor provides software (source or object code) that accesses NPERS data and is publically accessible, NPERS shall be allowed periodic access to conduct security code scans (i.e., Fortify SCA, AppScan) or NPERS shall be allowed access to review the results of scans conducted by the Contractor as part of their application development process. Contractor shall coordinate application vulnerability remediation plans with NPERS's IT Manager. Contractor shall include details on its application scanning process in the System Security Plan.
- Contractor shall maintain 24x7 Intrusion Detection and/or Prevention monitoring (IDS/IPS) using commercially acceptable tools or services. Contractor shall describe the details of the IDS or IPS in place to monitor the NPERS environment in the System Security Plan.

3. SPECIFIC SAFEGUARDS AND CONTROLS

Contractor shall maintain at least the following controls with respect to NPERS Data, consistent with Industry Standard Safeguards:

- Logical access controls to manage access to NPERS Data and system functionality on a least privilege and need-to-know basis, including through the use of defined authority levels and job functions, unique IDs and passwords, strong (i.e. two-factor) authentication for remote access systems, and elsewhere as appropriate, and promptly revoking or changing access in response to terminations or changes in job functions. Describe these controls in the System Security Plan.
- Password controls to manage and control password complexity, expiration and usage for all user accounts associated with access to NPERS Data, whether directly or indirectly. Passwords are required to be complex with at least 8 characters and a mix of alpha, numeric, and upper/lower case. Passwords will be changed every 60 days and cannot be re-used for at least 10 generations.
- Physical controls to protect information assets from environmental hazards and unauthorized access, and to manage and monitor movement of persons and equipment into and out of Contractor's facilities where NPERS Data is stored, processed, or transmitted. These physical controls should be detailed in the System Security Plan.
- Operational procedures and controls to ensure technology and information systems are configured and maintained according to prescribed internal standards and consistent with ISO-27001/27002 Standard Safeguards. Contractor shall "harden" all servers and network devices that access, store or process NPERS information. Contractor is required to document the settings of these hardened devices and test the device for compliance. Reports of configuration settings shall be delivered to the NPERS IT Manager upon reasonable request.
- Application security and software development controls designed to eliminate and minimize the introduction of security vulnerabilities in any software developed by Contractor for NPERS.
- Network security controls, including the use of firewalls, layered DMZs, and updated intrusion detection/prevention systems to help protect systems from intrusion and/or limit the scope or success of any attack or attempt at unauthorized access to NPERS Data. NPERS Data must be secured by at least two layers of firewalls, preferably from different Contractors, at all times and must have 24X7 IDS monitoring in place. Contractor will include a diagram of network security controls and boundary protection in the System Security Plan.
- Remote access to NPERS data is prohibited at all times, unless approved in advance by the NPERS IT Manager. All access to NPERS data must originate from equipment that is managed and controlled by Contractor's security policies and configuration settings. Personal equipment shall not be allowed to access NPERS information. Remote access using a secured VPN connection and two-factor authentication may be allowed if approved by the NPERS IT Manager.
- Wireless access to any NPERS data is prohibited, unless approved in advance by the NPERS IT Manager. Wireless networks within the Contractor environment shall be segregated from any networks that contain NPERS data, and shall be detailed in the System Security Plan.
- NPERS information may not be included on any type of physical or logical removable media, including paper, laptops, smart phones, disks, thumb-drives, or any type of data transmission (such as email). NPERS data shall not leave Contractor's internal network unless it is fully encrypted per NPERS requirements and approved by the NPERS IT Manager.
- Vulnerability management and Patch Management procedures and technologies to identify, assess, mitigate and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code. Contractor shall implement a periodic vulnerability scanning and process at least monthly, and track the remediation of all vulnerabilities through a corrective action process. Contractor shall implement a patch management process that runs at least weekly. Vulnerabilities and patches shall be corrected or mitigated in a timeframe that is commensurate with the priority of the security gap. Contractor shall describe these processes and priority settings in detail in the System Security Plan.
- Log collection and monitoring of System and Network Auditable Events" related to NPERS data and its protection. These events include, but are not limited to, setting of system time, log file updates, system and network startup and shutdown, system updates, hardware changes, initiation or acceptance of network connections, firewall modifications, and detection of suspicious or malicious activity from the

IDS or IPS. All logs shall be retained for one year. Audit logs shall be treated as highly confidential information with commensurate access controls.

- Encryption of NPERS Data in accordance with the requirements as set forth in the Encryption section of this document and using algorithms and key lengths consistent with Industry Standard Safeguards to reasonably protect NPERS Data against unauthorized access, disclosure, or theft during transfer or storage, and as defined in this Agreement.
- Asset Management process to track all inventory of equipment with access to NPERS data, including serial numbers and user ID assigned to the equipment if applicable. Inventory management will track all equipment from operational rollout through destruction, including any reassignments or maintenance outages. Contractor will describe the asset management process in detail in the System Security Plan. Contractor will provide NPERS a report of assets with access to NPERS information on request.
- Secure destruction or return of all NPERS Data prior to sending any unencrypted hard disk, portable storage device, or backup media offsite for maintenance, repurposing, or disposal purposes. Contractor will maintain NPERS information in its files or on its system only for as long as it is relevant or useful to the Contract. When this contract expires or is terminated, all NPERS Information, including files, removable media, and hard copies in the Contractor's possession are to be destroyed or returned to NPERS. Contractor must provide a written attestation to the NPERS IT Manager that all the NPERS information, including files and tapes, have been destroyed or returned to NPERS's IT Manager in accordance with all terms of the Contract.
- Maintenance and Currency of hardware and software. All critical hardware and software that support the NPERS business shall be maintained according to Contractor specifications and software shall remain within three versions of current release levels. Contractor shall not let any hardware or software that supports the NPERS business become unsupported. Support levels shall be documented in the Contractor Asset Management process.
- Disaster Recovery and Business Continuity planning that address the continued operation of all infrastructure, networks, and business operations related to fulfillment of this contract. These plans must be submitted to the NPERS IT Manager within 3 months of Contract execution and annually thereafter. All plans that related to NPERS data must be tested annually with at least a coordinated Table Top test.

4. CONTRACTOR ACCESS TO NPERS NETWORK AND SYSTEMS

To the extent that NPERS grants Contractor access to NPERS's computer network and/or telecommunications systems ("NPERS Network"), the following terms apply:

- Contractor's authorization to use the NPERS Network is specifically conditioned upon compliance with any technical requirements in the Contract Documents, including this Policy, and as may be provided to Contractor by NPERS in writing with respect to the access method. Contractor shall not cause, permit, or authorize any change, modification, enhancement, or additions to such technical requirements without the prior written consent of NPERS.
- NPERS reserves the right to monitor, inspect, or access Contractor's computer systems or other source devices when such devices are actively connected to or communicating with NPERS's Network or equipment, and intercept Contractor's communications traversing the NPERS Network or equipment at any time and without prior notice.
- NPERS may impose technical requirements or limitations upon the Contractor's access and/or the Contractor's computer systems which access the NPERS Network. These include requiring the assignment of permanent IP address(es) to the Contractor's computer(s) which communicate with the NPERS Network or equipment, as well as requiring the Contractor to provide to NPERS the names of Contractor personnel assigned to perform the services.
- Contractor shall notify NPERS as soon as is reasonably practicable, of any changes in such Contractor personnel in order to permit NPERS to promptly revoke access of Contractor personnel to NPERS's systems and NPERS's Network. If NPERS grants Contractor access to the NPERS Network via

Contractor's computer or other Contractor access device, Contractor agrees that prior to beginning such access it will have installed and activated up-to-date security products on such device, including but not limited to a host firewall and comprehensive anti-malware software (including virus and spyware protection). If Contractor becomes aware of any security issue (e.g. malware infection) with its access device when connected to the NPERS Network, Contractor shall promptly disconnect and notify NPERS.

5. NPERS NETWORK ACCESS RESTRICTIONS

Contractor may access the NPERS Network and associated applications solely for the purpose of providing designated services to NPERS. Contractor shall not use the NPERS Network, directly or indirectly, for any of the following purposes:

- to transmit to or receive from or communicate with networks, persons or entities other than NPERS and its officers and employees, except with prior written consent of NPERS (for example, one Contractor location may not use the NPERS Network to communicate directly or indirectly with other Contractor locations);
- to establish a peer to peer network connection between the Contractor's computer and any computer on the NPERS Network, the Internet, or Contractor's own network, without NPERS's prior written consent;
- for any unapproved use, including third party email or file transfer services (e.g., Hotmail, Yahoo, AOL, etc.) or to conduct any kind of unapproved business or transaction other than with, or for the benefit of, NPERS;
- to access, copy or store any confidential, proprietary, private or Personal Data;
- to accomplish any illegal or unlawful purpose, or to do any activity which would violate any law, rule, regulation, ordinance, or decree of any governmental authority, or cause NPERS to be in violation of any such law, rule, regulation, ordinance, or decree, or which could subject NPERS to any sanction, civil or criminal;
- to access any data and/or network to which Contractor does not have prior authorization from NPERS;
- to upload, post, email, otherwise transmit, or post links to any material that contains malicious software, bots, viruses, spam, time bombs, trap doors, or any other computer code, files or programs or repetitive requests for information designed to intercept, transmit, or otherwise gain unauthorized access to information or to interrupt, destroy or limit the functionality of the NPERS Network, telecommunications equipment, or data, or any other party's network, or to diminish the quality of, interfere with the performance of, or impair the functionality of the NPERS Network or any other party's network.

6. DATA ENCRYPTION REQUIREMENTS

To the extent applicable, Contractor shall encrypt all NPERS Personally Identifiable Information (PII) Data in transit and at rest using technology equivalent to AES 256. To the extent Contractor cannot comply with this requirement, Contractor shall provide notice to NPERS and the parties shall work together to develop mitigating procedures or schedules for encryption acceptable to NPERS. In the absence of prior express written permission from NPERS, Contractor shall not store PII on any portable storage device unless it is fully encrypted AND approved in advance by the NPERS IT Manager. Contractor shall maintain a key management plan that shall be approved by the NPERS IT Manager for any deployed encryption of NPERS data.

7. SECURITY AUDITS AND INSPECTIONS

- Contractor will provide NPERS, upon request and as applicable to the protection of NPERS Data, a summary report of any technical or procedural security assessments, vulnerability assessments, audits, and security inspections it has completed within the prior twelve (12) months, including a description of any significant (i.e. moderate or greater) risks identified and an overview of the remediation effort(s) undertaken to address such risks.

- Upon request and with advance notice, Contractor shall allow NPERS representatives reasonable access to its physical locations as necessary to review Contractor's system security environment and ensure all information security practices comply with NPERS requirements, Contractor personnel are appropriately trained in protecting NPERS data, and NPERS data is used for authorized purposes only.
- Contractor shall provide evidence of security gap tracking and action planning as a result of any review, audit, or assessment. NPERS understands the sensitivity of this information, and only requires access to security review findings and action planning directly involving NPERS information.

8. EXCEPTIONS AND CHANGES

NPERS understands that Information Security is a never-ending evolution of technology, processes, and procedures and there are many ways to mitigate security risks. As such, it is recognized that at times it may be impossible or impractical to comply with all aspects of this Security Exhibit. In those cases, Contractor shall provide evidence of alternative mitigating security controls or prepare a request for exception to the specific requirements. This must be submitted to the NPERS IT Manager for approval in advance of implementation of the requested exception or alternative security control. NPERS reserves the right to modify this policy as required.

If the Contractor is unable to meet the requirements of this section at the time the Contract is executed, the Contractor must work with NPERS to develop a compliance plan to be approved by NPERS for meeting these requirements and for putting in place compensating controls deemed necessary by NPERS. If a conflict exists between NPERS and Contractor's security protocols, NPERS and Contractor shall work to find a mutually agreeable solution.

Failure to reach agreement on security controls to be implemented as required by NPERS may result in termination of this agreement and Contractor requirement for return or destruction of all NPERS data.