Vendor Company Name:

NRG Contact:

Vendor Contact:

Description of Service provided by Vendor:

Date:

Vendor Security Criteria and Questionnaire

1. Overview

This document defines the minimum security criteria that a Vendor must meet in order to be considered for use by NRG Energy, Inc. As part of the Vendor selection process, the Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the seven categories. We will closely review the vendor responses, and will require remediation measures in any areas that fall short of the minimum security criteria. NRG Energy, Inc acceptance/approval of any given Vendor's information security profile depends largely on the vendor's response to this document.

These Standards are subject to additions and changes without notice by NRG Energy, Inc.

2.0 Scope

This document can be provided to Vendor's that are either being considered for use by NRG Energy, Inc, or have already been selected for use.

3.0 Responding

NRG Energy, Inc is looking for explicitly detailed, technical responses to the following statements and questions. Vendor's should format their responses directly beneath the Standards (both questions and requirements) listed below. Please include any security whitepapers, technical documents or policies that you may have that may assist us in understanding your information security profile.

Answers to each Guideline should be specific and avoid generalities – **Examples:**
Bad: "We have hardened our hosts against attack." *Good: "We have applied all security patches for Windows 2008R2 as of 4/30/2013 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (23:00hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to NRG Energy, Inc."*
Bad: "We use encryption." *Good: "All communications between our site and NRG Energy, Inc will be protected by IPSec ESP Tunnel mode using 256-bit AES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."*

4.0 Standards

4.1 General Security

1. NRG Energy, Inc reserves the right to periodically audit the *<Vendor Company Name >* application infrastructure pertaining to the environment hosting NRG Energy, Inc applications/instance to ensure compliance with the NRG Energy, Inc Information Security Policies and these Vendor Security Standards. Non-intrusive network audits (basic port scans, etc.) may be performed randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 48 hours notice.

2. The Vendor must provide a proposed architecture document that includes a full network diagram of the NRG Energy, Inc Application Environment illustrating the relationship between the Environment and any other relevant networks. Please include a full data flowchart that details where NRG Energy, Inc data resides, the applications that manipulate it, and the security thereof.

   Response:

3. Please describe where the data is stored? If it is hosted on a cloud storage service, please provide the service provider's name.

   Response:

4. The Vendor must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

   Response:

5. Please describe your Intrusion Detection Systems for both Host IDS and Network IDS.

   Response:

6. Please describe your processes regarding security incident response. If you have documented Incident Response Guidelines or Polices, please provide that as well.

   Response:

7. What is the Breach Notification process back to NRG Energy? NRG requires notification within 24 hours.

   Response:

8. Does the Vendor have a current Statement on Auditing Standards (SAS) 70 / SSAE 16 Report? If so, who performed the audit?

   Response:

9. If the Vendor does not have a current SAS 70 / SSAE 16 Report, does the Vendor meet other certified standards? (Please list the certification standard met, e.g. BSO, ISO, CMM, PCI and who performed the certification.) The Vendor shall provide NRG Energy, Inc copies of current and subsequent certifications. During the contract period, the Vendor shall disclose to NRG Energy, Inc any material weaknesses, or deficiencies

identified during audits on the Vendor facilities hosting, or data pathways, supporting NRG Energy, Inc projects.

Response:

4.2 Physical Security

1. The equipment hosting the application for NRG Energy, Inc must be located in a physically secure facility, which requires badge access at a minimum.

   Response:

2. The infrastructure (hosts, network equipment, etc.) hosting the NRG Energy, Inc application must be located in a locked cage-type environment.

   Response:

3. If NRG Energy, Inc Infrastructure is hosted, NRG Energy, Inc shall have final say on who is authorized to enter the physical environment containing the Application Infrastructure.

   Response:

4. The Vendor must disclose their access control procedures, including who amongst their personnel (by roles) will have access to the environment hosting the application for NRG Energy, Inc and their user administration processes.

   Response:

5. NRG Energy, Inc requires that the Vendor disclose their employee/contractor background check procedures and results prior to NRG Energy, Inc granting approval for use of a Vendor. Background check process must include confirmation back to NRG Energy, Inc that personnel working on our account have a clean background check.

   Response:

4.3 Network Security

NRG Energy, Inc requires a proof of a 3rd party external network and application penetration test to be performed on an annual basis or after a major network architecture change. NRG Energy, Inc needs proof of the penetration test results. Results are to be sent over secure transfer method to NRGInfosec@nrgenergy.com

Response:

1. Please describe your processes regarding network vulnerability management. If you have documented procedure, please provide that as well.

   Response:

2. NRG Energy, Inc requires that the network hosting the production and development environments be on separate (air-gapped) networks from each other.

   Response:

3. NRG Energy, Inc prefers that the network hosting the production application and data be air-gapped from any other network or customer that the Vendor may have. If this is difficult to achieve within the Vendor architecture, then please describe how NRG Energy, Inc's data is segregated from the data of other customers.

   Response:

4. NRG Energy, Inc requires access to any security, traffic or authentication logs relating to the access and connectivity to the NRG Energy, Inc's application and development environments.

   Response:

5. How will data travel between NRG Energy, Inc and the Vendor? Keep in mind the following three points:
   - If NRG Energy, Inc will be connecting to the Vendor via a private circuit (such as frame relay, etc.), then that circuit must terminate on the NRG Energy, Inc extranet. The operation of that circuit will come under the procedures and policies that govern the NRG Energy, Inc eCommerce Systems Management Group.

   - If, on the other hand, the data between NRG Energy, Inc and the Vendor will traverse a public network such as the Internet, the Vendor must deploy appropriate firewalling technology. The traffic between NRG Energy, Inc and the Vendor must be protected and authenticated by cryptographic technology. NRG Energy, Inc requires administrative access to any firewalls and/or routers on the NRG Energy's side of the firewall infrastructure.

   - No "split-tunneling" of any secure connection between the Vendor and NRG Energy, Inc.

   Response:

6. NRG Energy, Inc. has the right to randomly scan IP's of Vendor's who are collecting, processing, or transmitting NRG sensitive data.

   Website URL / IP(s):

   Response:

4.4 Host Security

1. The Vendor must disclose how and to what extent the hosts (Unix, Linux, Windows, etc.) comprising the NRG Energy, Inc application infrastructure have been hardened against

attack. If the Vendor has documentation for its hardening standards and processes, please provide that as well.

Response:

2. The Vendor must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.

   Response:

3. Does Vendor have antivirus software and malware installed and actively running with the latest pattern or virus signature file on all their servers?

   Response:

4. Information on how and when security patches will be applied must be provided. How does the Vendor keep up on security vulnerabilities, and what is the policy for applying security patches?

   Response:

5. The Vendor must disclose their processes for monitoring the integrity and availability of those hosts.

   Response:

6. The Vendor must provide information on their password policy for the NRG Energy, Inc application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

   - Password minimum requirements are:
   - Passwords must be a minimum of 8 characters long and comprise 3 or 4 types of categories (Upper case letters, lower case letters, numbers and special characters).
   - Temporarily lock accounts after 5 bad password attempts within 60 minutes, and lock for 30 minutes.
   - Passwords must be stored in an encrypted method (not plain text).

   Response:

7. NRG Energy, Inc. cannot provide internal usernames/passwords for account generation, as the company is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the Vendor authenticate users? (e.g., LDAP, Netegrity, Client certificates.)

   Response:

8. The Vendor must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

   Response:

4.5 Web Security

1. At NRG Energy, Inc's discretion, the Vendor may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).

   Response:

2. Please disclose whether, and where, the application uses Java, JavaScript, ActiveX, PHP or Vendor (active server page) technology.

   Response:

3. What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)

   Response:

4. Please describe the Vendor process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

   Response:

5. Has the Vendor performed a web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

   Response:

6. Has the Vendor performed an application penetration test? At minimum, testing against OWASP top ten web vulnerabilities.

   Response:

4.6 Cloud Security

1. What level (or tier) of service do you have with that provider (named in 4.1, question 3)? Please provide detailed information on the security services available for the tier of service with the cloud hosting provider.

   Response:

2. In the event of a breach at the cloud hosting provider, what are the notification times for the cloud hosting provider to notify you in case of said breach?

   Response:

3. How is the data transferred from NRG to the cloud? Is that data encrypted at rest and in transit?

   Response:

4. Does the Cloud Service Provider provide the capability to locate and search all of the customer's data? If yes, is this a supervised search capability or an unsupervised search capability?

   Response:

5. Does the cloud service provider allow a customer to select separate, specific location for the backup or replication of the data that still meets any of the customer restrictions on the nation/state level of location restrictions?

   Response:

6. In cloud databases, what mechanisms are provided for the customer to determine what columns are encrypted to prevent inference from non-encrypted columns?

   Response:

7. Does the CSP adhere to any established governance framework(s) involving data security controls?

   Response:

4.7 Cryptography

1. The NRG Energy, Inc application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the NRG Energy, Inc application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.

   Response:

2. Encryption algorithms must be of sufficient strength to equate to either, 168-bit TripleDES or 256-bit AES.

   Response:

3. Connections to the Vendor utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, SFTP.

   Response:

4. If the NRG Energy, Inc application infrastructure requires PKI, please contact NRG Energy, Inc Information Security Services for additional guidance.

   Response:

4.8 eCommerce

If the Vendor solution concerns any electronic commerce activities the following questions must be addressed:

1. Describe the protections for any transaction web pages hosted.

   Response:

2. Is any prospect or customer Personally Identifiable Information (PII) (ie., credit card, SSN. Drivers License, DOB, Bank Account, email) information collected and/or stored? Describe data collection method: paper or electronic.

   Response:

3. If credit card, SSN, Drivers License, DOB, Bank Account information is stored, is this information stored in an encrypted or otherwise protected manner?

   Response:

4. Is the application certified PCI – DSS compliant? (Please list the date(s) the certification standards were met, and who performed the certification.) The Vendor shall provide NRG Energy, Inc copies of current and subsequent certifications.

   Response:

5. Is the Vendor PCI-DSS certified? Is the Vendor a Tier 1, 2, 3 or 4 level merchant or level 1 or 2 service provider (for PCI-DSS classification purposes)? (Please list the date(s) the certification standards were met, and who performed the certification.) The Vendor shall provide NRG Energy, Inc copies of current and subsequent certifications.

   Response:

6. Please describe your processes regarding Data Retention, Data Deletion, and Data Deletion Certification process back to NRG Energy. If you have documented procedure, please provide that as well. This process should include phone recordings.

   Response:

4.9 HAN Device Security

If HAN devices are included as part of the Vendor solution the following questions must be addressed:

1. Please provide a system diagram showing communication paths to/from the HAN device including protocols and applicable TCP/IP ports.

   Response:

2. What specific measures are taken to prevent tampering with the device?

   Response:

3. How does the device provide access control or logical segmentation of consumer-specific data?

Response:

4. What encryption standards are used to secure data at rest and data in transit?

Response:

5. Are there any default accounts/credentials used to access the device? If so, how are these accounts secured following deployment of device?

Response:

5.0 Security - Other

1. Many of the applications and systems considered for this Vendor contain restricted, sensitive and private information, which NRG Energy, Inc is required to protect. NRG Energy, Inc is mandated to maintain its ability to ensure tight controls over the production and development environments and the information contained the databases.

2. Required Contract Clauses – NRG Energy, Inc Procurement Office must be notified if the applications and systems considered for this Vendor handle or store NRG Energy, Inc Restricted, Sensitive and private information, so that appropriate contract language is included. Examples of specific contract addendums typically used by NRG Energy are:
    - Credit Card Privacy – PCI Compliance Addendum
    - Personal Privacy – PII Compliance Addendum
    - Financial – Confidential Financial Information Addendum
    - HIPAA – Business Associate Agreement
    - General – Non-Disclosure Agreement