PRIVACY IMPACT ASSESSMENT (PIA)

PRIVACY IMPACT ASSESSMENT

Is this a new or substantially revised electronic information system? If revised, describe revisions.

- **This system, the Peace Corps Volunteer Application, is utilizing a new electronic information system.**

If any question does not apply, state not applicable (N/A) for each question and explain why.

I. Describe the information to be collected (e.g., nature and source). Be sure to include any information in an identifiable form, e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc).

- **The information is collected from the general public and includes: Name, address, date of birth, telephone numbers, social security number, email address, race, sex, national origin, ethnicity, education, financial obligations, legal history, drug and alcohol information, volunteer history, employment experience, essays, language skills, assignment and regional preferences, and other information relevant to the volunteer positions that Peace Corps provides overseas.**
- **This information, only when collected from the public in a hard copy of the application, will be scanned into the system by a Peace Corps staff person. Please note that this won't be necessary for the 99% of current applicants who complete Peace Corps Volunteer applications online.**

II. Why is the information being collected (e.g., to determine eligibility)?

This information is being collected in order to assess the eligibility of Peace Corps applicants, as well as to assess an applicant's technical competitiveness in relation to that of other applicants. This information is also being collected to assess the suitability of Peace Corps applicants, including their Cultural Sensitivity, Emotional Maturity, Motivation and Commitment, and Productive Competence (technical skills).

In addition…

- **Date of Birth, Place of Birth or Naturalization Number, and Intelligence Activities are necessary to determine eligibility for the Peace Corps.**

- **Email addresses are necessary to begin, save and submit the Peace Corps Volunteer application.**
- **Email addresses, Names, Social Security Numbers and Dates of Birth are used to verify the identities of individual applicants.**
- **City, State and ZIP code are used to track geographic locations of applicants for the purpose of analyzing application trends.**
- **Marital Status, Financial Obligations, Dependents and Military History are necessary to determine if there are legal or financial reasons why an applicant can not leave the United States for a 27-month Peace Corps assignment.**
- **References are collected in order to assess the suitability of Peace Corps applicants.**

III. How will the information be used (e.g., to verify existing data)?

- **See responses above.**
- **Additionally, Reason for Applying will be used to analyze what attracted applicants to the Peace Corps.**

IV. Will you share the information with others (e.g., another agency for a programmatic purpose)? If yes, list the entities.

- **This information is not shared outside the agency.**

V. Describe what opportunities individuals have been given to decline to provide information or to consent to particular use of the information (e.g., whether individual may withhold permission for a particular use).

- **A Privacy Act Notice will be provided which will indicate that providing the information is voluntary. However, failure to provide the information will preclude the successful submission of the Peace Corps Volunteer application.**

VI. How will the information be secured (e.g., administrative and technological controls)?

1. **Kenexa's architecture is composed of redundant firewalls with inline intrusion prevention modules (Cisco), switches (Cisco), load balancers (F5), web servers (HP/MS Windows Server 2003), application servers (HP/MS Windows Server 2003), search servers and database servers (HP/Windows 2003/SQL 2000). Kenexa maintains 2 redundant firewalls with inline intrusion prevention modules at the Internet perimeter and 2 redundant firewalls on the point-to-point T3 line between the corporate and hosted infrastructures. Firewall security policy limits in-bound perimeter access to essential Internet services necessary to access Kenexa application functionality and internal access on a host-by-host basis from Corporate to remotely manage the systems. All other types of traffic are strictly denied. Kenexa's IPS events are monitored and**

correlated 24/7 through Cisco Managed Services notifying Kenexa of any suspected attack.

Each server is "hardened" during a standard build process removing unnecessary services and patching before deployment. Patches are applied in approximately 45–60 days of release to remain in compliance with Kenexa's security certification requirements. Patches are immediately deployed to Kenexa's development environments as they are released by vendors. Once initial testing has been completed the patches are deployed to Kenexa's QA environments for full testing. Once approved patches are deployed to Kenexa's Staging, BETA, and Production environments. Web and Application servers can be pulled from their pools and patched without any customer impact. Database servers are patched during Kenexa's monthly maintenance (approximately 45–60 days after the patch was released). In the event of a critical patch where exploit code exists and could potentially impact Kenexa's environment these patches would be fast-tracked and emergency downtime would be scheduled for database patching.

Through Kenexa's separation of duties we ensure the principle of least privilege, by only granting the permissions required for an individual to perform his/her job function. Responsibilities are divided up between Kenexa's DBA, SCM, Hosting, Security, Corporate IS, Internal Applications, QA, and distinct engineering groups based on product (KRB, Gateways, and Workbench).

Each environment is segregated from the other and strictly controlled to ensure its integrity. Kenexa's environment consists of multiple development environments, multiple QA environments, BETA, Staging, and Production. Any change to the product follows a strict change control process where changes are first created in Kenexa's development environment. Once approved, they are moved to Kenexa's QA environments for thorough testing. Once the build has been officially approved by Kenexa's QA department it is scheduled and moved to Kenexa's Staging and Production environments.

All production servers have host-based IPS installed and real-time anti-virus with daily pattern file updates. Each physical tier has additional ACLs between them only permitting essential traffic for application functionality and support. The KRB web tier cannot talk directly to the database tier and the database tier does not have Internet access. Access to Kenexa's database servers is controlled at the server, database, application, and network level.

Kenexa limits any access to customer recruiting data to personnel with a business need to know. Kenexa has various security mechanisms in place to control access to those authorized. Anyone who has access to customer data is either an employee who signs a confidentiality agreement or, in very limited cases, a consultant or third party who has agreed contractually to protect the privacy of Kenexa's data.

For security reasons, Kenexa does not release lists of specific individuals who are provided access to customer data in connection with doing their jobs. But described below are various categories of

personnel who have access or might be given access for a specific business related purpose.

Personnel in Client Services & Support have access when needed to resolve a customer question or concern. Kenexa support personnel need access for program error reports and bugs to reproduce that bug in a customer specific environment because all Kenexa customers are individually configured. Without that data access, Kenexa cannot reproduce or fix the bug.

Personnel in Engineering and Quality have access in connection with the bug fixing and retesting process for the same reasons. Errors need to be reproduced in a customer environment and fixes need to be retested in the customer environment.

Kenexa internal ASP Operations and DBA Teams maintain all system operations and are the server/database administrators for all of Kenexa's clients. In that capacity, these personnel need access to all Kenexa's data and systems to make Kenexa's uptime commitments to customers and to perform maintenance.

Access to Kenexa's database servers is controlled at the server, database, application, and network level.

Redundant internal firewalls between Kenexa's Corporate and Production networks permit direct database access only to those who require permanent access to production databases for support purposes. This includes select members of Kenexa's engineering team in addition to Kenexa's Hosting Services, SCM and DBA teams. These individuals are located in a separate VLAN with network connectivity to both the Production and Disaster Recovery environments. Engineers requiring temporary access to the production environment are either temporarily moved to this VLAN or given temporary access via Kenexa's internal access portal to the production environment. All other traffic is denied with the exception of replication traffic between Kenexa's DR and Production environment and web connectivity to Kenexa's application. Access at all levels is reviewed on a monthly basis.

Once network access is granted, database access is granted by adding individuals to pre-defined groups granting the required read and/or write access to the database. Once an individual has completed his/her work this access is promptly removed and a new request must be made if access is again required.

All production server level access is further controlled utilizing RSA SecurID for two-factor Authentication. This access is limited to members of Kenexa's DBA, SCM, and Hosting Services Teams for support purposes.

Each client has a unique client ID. All data belonging to a particular client is uniquely identified via this ID.

KRB controls access to each client's data using this unique ID, ensuring that there can be no inadvertent access to, or release of, customer data to unauthorized (but valid) users of KRB.

Application access is controlled through Kenexa's centralized 'gatekeeper' process. Individuals with permanent access to a client's data include the helpdesk for customer support and the Client Services Consultant. Members of the engineering team may request temporary access to a client for a production support purpose. These are formal requests made to Kenexa's gatekeepers with the specific requirement for access. Each member has their own unique logon id and password. Once access is granted the individual only has access to the specific client they are working with. This access is removed once the work/project has been completed. Access by Kenexa users is logged within the application and specified as a Kenexa user with the corresponding individual's name. Audit trails are kept for edits to data in the database. These include the date and time the edits were made and the IDs of the users who made the edits.

The transport of all application information over public networks is protected using SSL. Customers may elect to utilize browser negotiated certs, which will connect at whatever strength the browser is capable of supporting from 40-bit to 256 bit SSL or at no additional charge.

In addition to the encryption utilized over public networks, KRB can encrypt specific fields within the database utilizing AES (256-bit) and passwords are hashed using SHA-1. Database backups are also encrypted before being put to media.

For Integrations utilizing FTP, Kenexa BrassRing offers PGP encryption, FTP over SSL, or FTP over SSH. XML based Integrations are done over SSL. AES private key or RSA public key encryption may be utilized to encrypt the integration payload.

Source code is available only within the Kenexa development organization and is controlled via StarTeam. Only non-critical JavaScript UI functionality is exposed in the client browser. All sKenexa'sce code within the organization is protected by multiple levels of authentication and network security.

Kenexa is Cybertrust Perimeter Certified and KRB is Cybertrust Application Certified.

For all applications, users must pass though a login screen and are assigned a unique username and password that is initially communicated by client assigned super user. This username/password combination is validated against values in Kenexa's database. The initial password must be changed at the first log-in. The super users assigned by the client add and inactivate users. User-id is 3DES encrypted and passwords are hashed using SHA-1. Users are able to change their passwords at any time while logged into the application. Kenexa also provides forgotten password recovery functionality on the log-in screen, which includes a Web-based query and e-mail response system. A 'forgot password' link is provided for users. Once the 'forgot password' link is selected and a user-id is provided, an email is sent to the email address currently associated with the user-id within the application. The email contains a URL to reset the user password. The URL expires after 8 hours.

When the password is changed the source IP address is captured and a notification is sent to the user stating that their password has been changed.

Session Encryption is set to 40/128-bit SSL and Gateways sessions can be encrypted with SSL.

Fields on forms in KRB can be AES encrypted. Generally, this feature is used for sensitive information, such as a social security number.

2. **The Peace Corps secures encrypted data in transit by transferring it via SSL.**

3. **The Peace Corps stores data at their headquarters-based datacenter using a separate subnet, separate managed network switch, and encrypted SQL server database.**

VII. How will the data be retrieved (e.g., will it be retrieved by a personal identifier such as name, social security number, address, telephone number or some other identifier that is unique to an individual)? Will a System of Record Notice be created under the Privacy Act, 5 U.S.C. 552a?

- **Data will be retrieved by applicants using an e-mail address and password that applicants have individually personalized and which is unique to an individual.**
- **System end users will be able to search and retrieve information based on a unique identifier assigned to each applicant by the Kenexa system, as well as searching by name or social security number. The medical system will also be searchable by a uniquely assigned case number.**
- **The data collected is currently maintained under a System of Records: PC-17-Volunteer Applicant and Service Records System.**