Security and Privacy Policy

Individually Identifiable Information
Aon Hewitt recognizes that the growth of online services has created many privacy concerns, particularly for consumers. These concerns focus on protecting "individually identifiable" information that an individual or customer reasonably expects to be kept private. As the term suggests, individually identifiable information is information that can be associated with a specific individual or entity, such as name, address, telephone number, e-mail address and/or information about online activities directly linked to them.

It is common practice and often a necessity for companies, governments or other organizations to collect individually identifiable information in order to conduct business and offer services. For example, a telecommunications provider may collect individually identifiable information in the course of billing and providing telephone service to a customer.

Aon Hewitt's Privacy Policy
Aon Hewitt has developed the following privacy policy to protect individually identifiable information. This policy covers Aon Hewitt and its subsidiaries and applies to all individually identifiable information that Aon Hewitt obtains when a customer provides eligibility substantiation documentation during the course of the verification.

Disclosure. Aon Hewitt will not sell, trade or disclose to third parties any individually identifiable information derived from the completion of an eligibility verification (except as required by subpoena, search warrant or other legal process or in the case of imminent physical harm to the customer or others). When Aon Hewitt uses other agents, contractors or companies to perform services on its behalf, Aon Hewitt will ensure that the company protects your individually identifiable information consistent with this policy. The results of these verifications, along with the substantiating evidence, may be provided to the benefit plan sponsor, or designated business associate during, or at the completion of the verification.

Collection and Use. Aon Hewitt will collect and use individually identifiable information for eligibility verification purposes, to provide assistance in complying with eligibility verifications, or to notify you about an upcoming or ongoing verification.

Security. Aon Hewitt has implemented technology and security features and strict policy guidelines to safeguard the privacy of your individually identifiable information from unauthorized access or improper use, and we will continue to enhance our security procedures as new technology becomes available. These policies include, but are not limited to; document access logs, secured physical storage facility with multiple lock access requirements, secured server facility, employee background checks, and advanced encryption techniques.

Aon Hewitt Information Security
Aon Hewitt maintains an in depth security policy that describes all necessary procedures to maintain a high level of ongoing security. The policy discusses password policies, security log procedures, classification of vital information and how it is to be encrypted and transferred as well as defines network security administrators who review and approve all of the above information.

Aon Hewitt encrypts all passwords. Minimum password length and complexity is enforced. Aon Hewitt utilizes roles-based security to ensure data confidentiality and security. Application users are only provided access to data on an as-needed basis to perform the functions related to their position. User authentication takes place via a backend process that validates user, client access, and password information.

Aon Hewitt takes system security, privacy, and reliability very seriously. The Aon Hewitt electronic delivery mechanisms are a key differentiator in the industry, and Aon Hewitt seeks to ensure high levels of availability of these systems. The Aon Hewitt strategy is to anticipate potential problems and resolve them in advance.

Security
Aon Hewitt has policies and procedures in place to address all recommended security incidents. We have alarms configured to notify us when any unauthorized network intrusions or other network security related events occur. We also have assigned personnel who check security logs on a daily basis for violations and anomalies. Clients would be immediately contacted and informed of the security violation, and Aon Hewitt would take all necessary steps to contain the problem. ID logs and other security transaction logs are used to identify invalid access attempts and other security related incidents, and to help us track down and resolve security related problems as required.

Log monitoring occurs on a daily basis with all vital data storage servers. Multiple contacts are notified immediately and emergency action procedures go into effect when an error is detected. Logs are backed up and stored offsite for future need as required.

We use multiple enterprise level products to manage and protect our data and users from malicious infections. We use an industry grade anti-virus server and software products to perform on demand and daily monitoring of worms and viruses. Software automatically updates virus definition files on a daily basis, and Aon Hewitt performs full weekly scans of all files and e-mails. Exception reports notify network administrators of any virus issues for immediate research and action. We also use industry recommended spy ware products to protect our web users from the influx of spam and spy ware.