



DEPENDENT VERIFICATION CENTER
P.O. BOX 1506
LINCOLNSHIRE, IL 60069-1415

Return Service Requested

0000-1-1 HAE2 13960634 03-21-2023

SALLY TEST

DO NOT MAIL

ANYTOWN, ONTARIO 00000

TIME SENSITIVE MATERIALS ENCLOSED



3/21/2023

ANNOUNCING THE GEORGIA DEPARTMENT OF ADMINISTRATIVE SERVICES - HUMAN RESOURCES ADMINISTRATION DEPENDENT ELIGIBILITY VERIFICATION

A RESPONSE WILL BE REQUIRED FROM ALL EMPLOYEES WHO COVER DEPENDENTS IN THE FLEXIBLE BENEFITS PLANS (the Plan).

In the coming months, employees who cover dependents in the active/retiree dental, vision, spouse/child life and/or the spouse critical illness plans will be asked to provide documents that validate that the persons enrolled are their legal dependents. To prepare you for the next step in this process, please locate marriage certificates, birth certificates or any other documents that you may need to verify your dependent(s). We know this process may be an inconvenience, but ALL dependents covered by the Plan will be documented for 2023 or coverage will be canceled. The Georgia Department of Administrative Services has a responsibility to all employees to ensure their plans are covering eligible dependents only.

Why is the Georgia Department of Administrative Services verifying dependents?

The Georgia Department of Administrative Services, by law, can only cover eligible employees and their eligible dependents. The dependent eligibility verification is necessary to ensure that the health plans are compliant with these laws. Allowing the coverage of dependents who are not eligible puts the company and all eligible employees at financial risk.

What is the verification process?

The Georgia Department of Administrative Services is working with Alight Verification Services, a dependent verification company, to verify dependents in the Plan. The Alight Verification Center will soon be asking you for copies of documents that prove any dependent you currently have enrolled in the Plan is, in fact, your eligible dependent. You may be asked to provide a copy of your marriage certificate, birth certificates, prior year federal tax return, court-ordered divorce decree and custody agreement, and other types of documents that verify your dependent(s). The Dependent Verification Center will follow up with you as necessary to complete the process. Once your dependent(s) have been verified by the proper documents, the copies you provided the Dependent Verification Center will be destroyed. **Remember — DO NOT PROVIDE ORIGINAL DOCUMENTS!**



You will be notified before any dependent is removed from coverage and be given an opportunity to provide additional information. However, your response to the verification request is required. If you do not provide documents that verify your dependent(s), coverage for any ineligible dependent will be canceled.

Who is an eligible dependent? Who is not?

Generally, your legal spouse and children under the age of 26 are eligible for coverage. In some cases, older children may also be eligible dependents. If you are unsure whether persons you are covering in the Plan are eligible, the Dependent Verification Center will be able to assist you in the process.



Security and Privacy Policy

Individually Identifiable Information

Alight Solutions LLC 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.

Alight's Privacy Policy

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

Disclosure. Alight 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 Alight uses other agents, contractors or companies to perform services on its behalf, Alight 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. Alight 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. Alight 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.

Alight Information Security

Alight 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.

Alight encrypts all passwords. Minimum password length and complexity is enforced. Alight 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.

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

Security

Alight 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 Alight 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 Alight 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.

