GREENSHADES SOFTWARE

GREENEMPLOYEE LOGIN SECURITY

WHAT IS NEXT FOR GREENEMPLOYEE LOGIN SECURITY?

Greenshades Software is taking proactive steps to increase the security of the GreenEmployee login process. The upcoming enhancements introduce stronger authentication options beyond traditional passwords. The changes include a new 2nd Level Identity Confirmation for the account setup process and 2nd Factor Authentication options for employee logins.

Changes made in March included requiring custom passwords for all logins. These changes successfully protected our client's employees, but we are taking our security enhancements further. In conjunction with an independent third-party security expert, we have designed these new features to proactively increase security for our clients. These enhancements are intended to protect against today's threats as well as future threats. threats.

Once released, all employees who have an existing account or wish to establish a new account on GreenEmployee will need to provide an email address. Of the planned improvements, requiring an email address for an account will have the largest impact to your employees. In order to ease the impact of this change, we are using a phased roll-out plan, detailed at the end of this document. In Phase 1, we will focus on collecting email addresses from employees currently using GreenEmployee. Phase 1 will be released and accessible to employees soon.

Through the entire process, employees will continue to use the same URL to log in. Employees that have already set up custom passwords will not be required to change their passwords. Employees will see clear information and instructions on the GreenEmployee portal as the changes are released, informing them of how the changes affect them.

At any time, employees without an email address will still be able to access their content without an account. However, employees without an account will be required to provide 2nd Level Identity Confirmation every time they attempt to access secure content.

We know that changes to the GreenEmployee portal can have a significant impact on you and your employees. This is why we are focused on making this transition as easy as possible while insuring that the security of the login process is improved. Thank you for your assistance and understanding. We hope this guide helps you plan for the upcoming changes. We intend to keep you updated as we begin each new phase. Please email our security team if you have any questions.

SECURITY FEATURES AND IMPROVEMENTS

There are a number of new features included in these upcoming releases that will increase the security of the GreenEmployee login process. Many of these features are configurable to suit your company's needs. We will release the new administrator settings for these features before we release the new features to your employees. This will allow you, as an administrator, the ability to establish your preferences before employees use the new functionality.

Please review these features and options with your IT or security representative to determine what is the most appropriate security configuration for your organization.

ACCOUNT SETUP AND ACCESS

Employees that currently have an account with a custom password will be able to login using their email address on file as their User ID. This is a change from their currently configurable User ID to always using an email address.

Employees that do not currently have an account with a custom password will be able to set up an account. To set up an account, an employee must provide a valid email address and custom password. Next, the employee will provide their Social Security Number or Employee ID, along with their Date of Birth to identify them in our system. The employee will then need to confirm their identity with our new 2nd Level Identity Confirmation (more on this below). Once the employee has set up an account and confirmed their identity, the employee will be able to login with their email address and password for all future logins.

You, as an administrator, will have the ability to restrict acceptable email addresses to certain domains. You will also have the ability to enforce minimum password complexity. Minimum password complexity options are already available through GreenshadesOnline.com. Please consider setting those to your preferences now.

As part of this change, GreenEmployee will require that each email address in our system be unique. It will also require that the employee has access to that email account before the employee is able to complete the account setup.

NO-ACCOUNT ACCESS

We understand that you may have employees that do not want to or cannot create accounts with an email address. In order to serve this population of employees, while not compromising their security, we are including a new No-Account Access option. The No-Account Access option requires the employee to provide their Social Security Number or Employee ID, along with their Date of Birth to identify them in our system. The employee will then need to confirm their identity with our new 2nd Level Identity Confirmation (more on this below) each time they access the system using the No-Account Access option.

2ND LEVEL IDENTITY CONFIRMATION

All employee access will require the employee to confirm their identity through a 2 step process. This 2 step process is only required once for account setup, but will be required every time for an employee utilizing the No-Account Access option.

First, the employee will provide their Social Security Number or Employee ID, along with their Date of Birth to identify them in our system (Step 1). Second, the employee will use one of the following identity confirmation options for a second level of identity confirmation (Step 2). All 2nd level identity confirmation options are configurable by you as administrator.

- Text a verification code to the employee's mobile number that the company has on file. The employee must retrieve this code and provide it to the portal.
- Have GreenEmployee call the telephone number that the company has on file for the employee to provide a verification code. The employee must provide this code to the portal.
- Email a verification code to the employee's email address that the company has on file. The employee must retrieve this code and provide it to the portal.

- Generation and distribution of secure access codes to employees via postal mail or other channel managed by you as the administrator. Employees will have to provide their specific access code to the portal.
- Have the employee call you to receive their secure access code. Employees will have to provide their specific access code to the portal.
- Use a separate admin account approval workflow where you, as the administrator, review and approve accounts via the administrative portal.
- Ask the employee a series of identity challenge questions that are setup by you, as the administrator.

2ND FACTOR AUTHENTICATION OPTIONS

2nd Factor Authentication requires the employee to know something (their custom password) and have something (a device such as a mobile phone or a previously authenticated computer). When an employee adds 2nd Factor Authentication, they will provide a mobile phone number to the portal. The mobile phone number will be used to send a verification code when the employee attempts to login. The verification code, which can only be received by that mobile phone, will then be required for login (2nd factor). During an employee login using a mobile verification code, we will also store the information of the computer that was used for a valid 2nd factor authenticated login. In the future, a login from that same computer, from that same location, can serve as the 2nd factor and will not require the mobile phone verification code.

These 2nd Factor Authentication options are completely configurable. The employee can turn on 2nd Factor Authentication for themselves. The employee can accept only mobile phone verification codes as a 2nd factor. Administrators can require 2nd Factor Authentication for all employees, and can choose only mobile phone verification codes as a 2nd factor.

This authentication process is separate from and in addition to the 2nd Level Identity Confirmation described above.

PASSWORD RESTRICTIONS

You, as an administrator, will continue to have the ability to expire passwords after a certain amount of time and prohibit the reuse of old passwords.

You will be able to lockout accounts if an employee has too many failed login attempts. Account lockout will change from an optional feature to a required feature, but you will be able to set the number of failed attempts before lockout.

IP ADDRESS RESTRICTIONS

You, as an administrator, will be able to restrict employee login access to only employees accessing from certain IP addresses or IP ranges. This will include the ability to restrict access to only United States IP addresses. You will also be able to report IP addresses which you believe are suspicious. Our security team will then investigate any IP addresses reported by our clients.

ROBUST EMAIL NOTIFICATIONS

Automatic emails will be sent to employees to notify them of all changes to their email address(es), passwords, and/or any configured 2nd Level Identity Confirmation fields. This will help alert them to any potentially fraudulent changes as soon as possible.

EMPLOYEE LOGIN HISTORY

Employees will have increased visibility on their most recent logins and login information. This will help them spot any fraudulent accesses as soon as possible.

INACTIVITY TIMEOUT

You, as an administrator, will continue to have the option to log employees out after a period of inactivity. On logout, employees will now be automatically redirected to the login screen.

COMPANY SEARCH

You, as an administrator, will have the ability to remove your company from the company search results. This will limit access to only those employees who know your company code.

TENTATIVE TIMELINE

The exact timeline for these changes is being developed. We are planning to release the changes in phases in order to make the transition as easy as possible.

PHASE 1: PRE-TRANSITION

During this phase, Greenshades will be releasing changes for employees and administrators in order to ease the transition to the new login methods and authentication options. The main goals of this phase are 1) to ensure that all active employees with an account will have an email address prior to Phase 2, and 2) administrators are able to establish settings for new features prior to Phase 2. Phase 1 began on July 5, 2016.

WHAT SHOULD EMPLOYEES EXPECT DURING THIS PHASE?

Upon successful login, employees will be asked to provide and confirm an email address that will be used in the future as their User ID. The email account will be sent a verification code, which must be entered on GreenEmployee to confirm the employee has access to that email account.

Prior to moving to the Phase 2, employees will be reminded of the email address they confirmed since it will be used to login in the future.

WHAT SHOULD ADMINS EXPECT DURING THIS PHASE?

Over the course of this phase, administrators will begin to see additional and improved options in the Employee Access settings on GreenshadesOnline. These new options will exist alongside the current settings and will allow you to configure options for the new features before they are released to employees in Phase 2.

PHASE 2: TRANSITION

This phase will begin when a new login page is released. Employees will no longer be asked for their previously configured User ID, but will instead be required to login using their email address and custom password. As a transition phase, employers can choose to migrate to the new pages. Phase 2 began on August 28, 2016.

WHAT SHOULD EMPLOYEES EXPECT DURING THIS PHASE?

- An employee should expect to see a slightly different login page. It will ask for an email address and custom password, instead of their current User ID and custom password. It will also have an option for No-Account Access, if the employee wishes to continue without an email address.
- An employee that has not yet updated their account with an email address will be required to do so prior to logging in through the new login page.
- An employee attempting to reset their password will be required to use the 2nd Level Identity Confirmation process. They will no longer be able to reset their password using the current process.
- An employee will have the option for No-Account Access. They will need to complete the 2nd Level Identity Confirmation process each time they use No-Account Access.
- An employee accessing the GreenEmployee portal for the first time will be required to set up an account using the new process (email address, custom password, and 2nd Level Identity Confirmation) or using the No-Account Access option.

WHAT SHOULD ADMINS EXPECT DURING THIS PHASE?

During the Transition Phase, employees may have questions about the updated login process and may have questions about the configuration you have chosen for the company.

Depending on the 2nd Level Identity Confirmation options enabled by the administrator, some employee account setup and No-Account Access workflow may involve administrator approval and/or involvement.

PHASE 3: CONVERSION

At the end of Phase 2, Greenshades will remove the option to login with the old login method (using the previously configured User ID) and will completely convert to the new account login process. Phase 3 will begin on December 1, 2016.

WHAT SHOULD EMPLOYEES EXPECT DURING THIS PHASE?

- An employee will be required to login with the new login method only. This means they will need to have an email address and custom password account or use the No-Account Access option.
- An employee that has not yet updated their account with an email address will be required to do so prior to logging in.
- An employee accessing the GreenEmployee portal for the first time will be required to set up an account using the new process (email address, custom password, and 2nd Level Identity Confirmation) or using the No-Account Access option.
- An employee will have the option to enable 2nd Factor Authentication for their account, including options that require mobile number text verification only.

WHAT SHOULD ADMINS EXPECT DURING THIS PHASE?

There may be enhanced options that will be completed and released in this phase.

PHASE 4: ENHANCEMENT

Providing the best security for our clients is a continuous process and requires that Greenshades continue to stay on top of industry best practices and ahead of security threats. Therefore, we will continue to enhance the employee login pages and options beyond the first 3 Phases presented here.