GA@WORK

Change Impact View

Security

GA@WORK

As of date: 05.21.25

PERSONA DESCRIPTION

- The change impact information included is most applicable to **Agency Security Partners (ASP)** (this role was called Agency Security Officer in TeamWorks) and **Identity Provider (IdP) Administrators**.
- Each State of Georgia agency will assign a primary and secondary ASP who is responsible for managing Security Request Forms to grant access to agency users. ASPs are final access approvers for their agencies.
- The information on this change impact view is not exhaustive, and users are reminded to complete applicable training and review Job Aids.

KEY CHANGES FOR ASPs

- Managers now have access to view and submit security requests outside of their own agencies. To avoid errors, Managers and ASPs should ensure an additional review when submitting security requests in GA@WORK, confirming they are only submitting within their own agency.
- The ASP or Manager will submit a security request in GA@WORK using one of seven specific forms based on the security need. The ASP will review and approve the request. GA@WORK will notify the State Accounting Officer (SAO) Security team for processing. The team will subsequently provide, approve, or provision the necessary access. Once access is granted, the ASP will receive a notification in their Inbox in GA@WORK.
  - **Note**: Not all seven request forms are applicable to every agency.

DELEGATION OF AUTHORITY

- Delegation of Authority allows a user to assign work tasks to other agency personnel such that work continues in their absence.
- Examples of activities that can be delegated include expense approvals, time off requests, and performance reviews.
- Agency Security Partners are responsible for reviewing and confirming the delegation of authorities submitted by their agency personnel in GA@WORK.

KEY CHANGES FOR IDPs*

When an individual is hired or terminated, HR will now be required to share the employee ID with the IdP Administrators. Once the IdP Administrator receives the Employee or Contingent Worker ID, the IdP Administrator will need to grant, set up, or remove Single Sign-On (SSO) access.

- **Note:** *This change specifically applies to the ~25 agencies using SSO, referred to as SSO agencies.

What are benefits for Security in GA@WORK?

- The Delegation of Authority feature helps make sure work goes on if an approver goes on leave.
- There is automatic removal of access when an Employee is terminated.

What could be challenges to Security to adopt GA@WORK?

- There is a new process for IdP Administrators for managing system login access for employees in agencies using Single Sign-On (SSO) and native Login with Multi-Factor Authentication (MFA).
  - A thorough review of an employee's information will be required when onboarding and transferring from agency-to-agency to ensure the correct person is added or moved.
  - Before go-live, users must know how to access GA@WORK. It will be covered in training.
- When submitting security requests within GA@WORK, a total of up to seven types of security request forms may be available in GA@WORK, and attention must be taken to select the correct form.
- Each ASP is required to have their security request forms reviewed by their fellow ASPs before submission to the State Accounting Office (SAO) Security team.
  - This peer review process ensures the accuracy of the forms, preventing errors such as submitting forms for incorrect agencies or individuals.

What is not changing?

- ASPs will continue to have the ability to reset passwords and lock user accounts for their agencies
- The completion requirement of Quarterly/Annual Segregation of Duties (SOD) account reviews for ASPs

Note: Failure to complete attestations will result in a report of non-compliance to the State Accounting Officer.

MORE INFO | https://sao.georgia.gov/nextgen