PolicyStat User Roles and Permissions

PolicyStat User Roles and their associated permissions are one of the three Pillars of PolicyStat. These settings determine not only the actions a user can take across the site, but also what responsibilities they have.

The Guest role is not technically a role you assign. Site Administrators can generate what is called a Guest Access link to allow users to access PolicyStat without the need to sign in. Guests can search and view non-restricted, active policies across the site. However, Guests cannot be assigned acknowledgments or elevated permissions, as there is no way to identify who they are. Access via a Guest Access link is noted by one of these identifiers.

Next up is users. Users have basic access to search for and view any non-restricted, active policies across the site. Users can be assigned policies to acknowledge or elevated permissions. Access as a user requires a login but depending on your local settings this may require synching with Active Directory or utilizing Single-Sign On to bypass the need to enter a username and password.

Users can be granted permission to view policies that have been set as restricted. For example, if a policy should be visible to specific Human Resources personnel, the policy settings can be modified to restricted and only users with View Restricted permission levels or higher for the HR Area will be able to locate and see it.

Members of an Approval Workflow are considered Approvers. In addition to marking their approval of a policy, Approvers can edit or modify a policy while it is pending through the Workflow.

Owners are the users ultimately responsible for a policy, often including making initial edits during the review and then kicking off the approval process. An Owner may have been the one to create the original policy, but do not necessarily need to be.

Users can also be assigned as an Area Editor, a role which can create new policies and edit any existing policies. This role can be assigned either by Area, or site-wide if desired.

Users can also be assigned as Area Managers, with the same Editor permissions, but also manage an Area. Area Managers are typically managers or supervisors who require the ability to oversee action on policies within their department. They receive notifications for actions taken on any policies within their respective area. Area Managers can also assign acknowledgments for any policies they manage. This role can also be assigned site-wide.

Finally, Site Administrators manage and administer the entire site. They have access to all the features of PolicyStat across site and oversee both user and workflow management. If you are part of a system, this role can be assign for every location or only specific sites.

For standard users, your local site administrator is your first line of defense when encountering issues within PolicyStat.