



CORE

Colorado Operations Resource Engine

FAQs

Your Questions about CORE

Volume 9: Security

Click below to find all
the FAQs:

<https://www.CoreFAQs>

Contact us at

core.news@state.co.us

How does Security work in the CORE system?

CORE Security is the process that enables end users to access appropriate documents, tables, or queries they need to perform their job tasks. Equally important, the security restricts their access to update other system pages not related to their role. Security is governed by roles. Employees are assigned to roles based on their job functions. A user who does not approve a document may still have access to view it. Roles are assigned to each user by department code.

Who decides and sets up the roles and approvers?

In March 2014, all departments provided data to identify who in their departments performs various tasks associated with specific security roles. For example, employees who enter purchase requisitions (RQS) were 'mapped' to a Procurement Requisition Entry role in the system. That role allows them to enter purchase requisitions for their assigned department(s). Many State employees have been assigned multiple roles in CORE.

Departments also indicated who in their departments should have the ability to create documents, approve documents, update tables, or view only. At the highest level, the current Security Administrators, typically the department Controllers, approved the roles assigned to CORE users in their department.

Is there a limit to the number of security roles?

CORE has standard roles and there is not a limit for defined roles. Colorado has purchased an enterprise license and each department has enough to assign its end users.

What are the types of access in CORE?

ACCESS TYPES	<ul style="list-style-type: none">• View / Inquire – Look at a document, table, or query in Read Only status.• Add / Update - Create a new document, change an existing document, or modify a table.• Approve – Move a document from pending to an approved status
--------------	--