TSB SCCOE Information Systems Security

Scope

The management and maintenance of accounts is an important task that is shared by the Technology Services Branch of Santa Clara County Office of Education and by the Districts that use these systems. This procedure describes the request and approval process for obtaining privileges for a role based account.

Philosophy and Principles

- The principle of least privileges applies: To the extent possible, accounts should be granted sufficient privileges to perform the approved business function and no more.
- Accounts for individuals and the passwords to those accounts ***may not be shared*** except in the case of information only accounts granted to a district.
- All requests must be reviewed and approved from both a business and technical perspective. The business approval confirms that the account requested is needed to perform a required business function. The technical approval confirms that the privilege requested is required to achieve the approved business need.
- Separation of duties must be maintained: The person with the authority to approve a request should not be the person that fulfills the request.

Roles

- TSB District Authorized Signer – approver representing the district.
- TSB Data Trustee – TSB staff assigned to security duties with escalated system access.
- Account Owner – Person responsible for acceptable use of system access.
- AccessPoint Service Request – All requests for assistance and support are managed through the AccessPoint at Accesspoint.sccoe.org. Customers may enter Service Requests and attach forms to Service Requests.
- System Security Form – form used for adds, changes and inactivations of system access. This form is available on AccessPoint and must be signed by the TSB District Authorized Signer.

Technology Services
Santa Clara County Office of Education

TSB District Authorized Signer Designation

- Each fiscal year TSB sends a signature card to the Superintendent of each District to identify who can approve system security changes and authorize individual accounts for the district.
- Districts may have more than one TSB District Authorized Signer.
- The TSB District Authorized Signer is independent of the District Authorized Signer maintained by other Branches of SCCOE. However, he or she may be the same person.
- The TSB Authorized Signer assumes responsibility for maintaining good computing practices at the district in alignment with the TSB Business System Security philosophy and principles.

General Account Management and Life Cycle

Account request and provisioning

- New account/change request is made by completing the TSB Security Form with the signature of an authorized approving the request. TSB recommends that each request be reviewed by the immediate manager in the business unit of the district, as well as the authorized signer.
- Account Owners external reference number/employee ID from QSS is required on the security form.
- TSB Security Form is reviewed and signed by the TSB District Authorized Signer.
- TSB Security Form is scanned and attached to an AccessPoint Service Request.
- TSB Help Desk reviews the AccessPoint Service Request for completeness and forwards the request to the appropriate TSB team.
- TSB Data Trustee reviews and authorizes the request if there are no exceptions to existing roles and TSB Security Philosophy and Principles.
- TSB Data Trustee executes the request.
- Email with new account is sent to the Account Owner.
- The temp password is provided to the Account Owner by phone and the system prompts to change password on login.

Technology Services
Santa Clara County Office of Education

Annual Account Access Audit

At the end of every fiscal year TSB District Authorized Signers are provided a list of current account holders to review and update access.

Account Inactivation

- It is the TSB District Authorized Signer's responsibility to notify TSB when an account should be closed.
- TSB should be notified to close an account within 24 hours when account holders have elevated security and/or approval.
- TSB Data Help Desk will remove access within 3 business days unless otherwise requested, or elevated security exists.

Exceptions

Occaisionally there may be a business need that requires an exception to the philosophy of least system access and seperation of duties. In that case TSB requires the TSB District Authorized Signer to approve an Security Exception Form.

TSB data trustee will complete the exception form with detailed information. The TSB data trustee may escalate security concerns to the Manager, Director or CTO for further review.

TSB District Authorized Signer approves the form and accepts responsibility for monitoring and managing the system access that is outside normal practice.

District Responsibilities

Districts must include acceptable use policies in their employee agreements that are in alignment with TSB Business System Security Philosophy and Principles. Districts are responsible for maintaining a TSB District Authorized Signer and determining the District's internal process.