

Cal Net Technology Group Scope of Work - System Lockout

Company Name: [Client Company Name]

Site POC:

Technical POC:

Project Name: System Lockout

Business Objective: Protect intellectual property and maintain security through the change of critical system passwords and disabling of access when company switches I.T providers or internal I.T. employees separate from the company.

Req. Completion Date: [Date of Lockout]

Revision History

Date	Version	Author	Details
1/25/2009	1.0	Cal Net	First draft

Pre-Planning Steps

1. Acquire all user names and passwords of all critical systems. (See checklist example)
2. Test all access per the checklist to ensure accuracy.
3. Review service accounts on all servers to ensure that the user's account or domain administrator account is not used so the password change does not take down a critical system. Create service accounts and change services as necessary.
4. Acquire all contact information for 3rd parties that need to be notified.
5. Communicate with upper management when the date of separation will be.

Lockout Day

1. For terminations, have an engineer be onsite at the time that the I.T. provider or employee will be terminated and escorted off the premises, if I.T. provider or employee is currently on premise.
2. For voluntary separations, the procedure will be done as of the end of the last working day of the I.T. provider or employee.
3. The engineer will begin changing perimeter system passwords first; disable the user's account, etc., per the checklist.
4. The engineer will begin testing each system to ensure they still function.
5. If there are any services that cannot be changed immediately, because it would be detrimental to company business, the systems will be changed according to a time determined by the client.
6. After all systems are changed and tested, inform the client that the work is completed.

Post-Lockout Day

1. Have an engineer be present the first day after the lockout to ensure all systems are running smooth.

Client: _____

Date of Lockout: _____

Affected Personnel: _____

Eng. Performing Lockout: _____

Primary Site Contact: _____

Primary Site Phone# _____

Site: _____

Order	System Name/Type	Description	Site/DNS Name/IP	Login Acct Name	Old Pwd	New Pwd	Contact #	Contact Name	Acct# (if appl)
1) Disable Admin Access									
	Network Access	Disable admin's user account							
	Group Access	Remove account from internal groups/lists							
	Reroute email	Attach old email address to supervisor's mailbox							
2) Perimeter Equipment									
	Router								
	Firewall								
	VPN								
	Anti-Spam								
	IP KVM / iLO								
	Wireless	WAP info							
3) Public-Facing Systems									
	Public Website	Mgt. of public website, if hosted							
	Network Solutions	Mgt. of domain registration site							
	GoDaddy SSL Mgr	Mgt. of SSL Certificates, if separate							
	DNS Mgr Site	Mgt. of DNS names, if separate							
	Other public system	Mgt. of others such as alarms, phones, alerts, etc.							
4) Users									
	Domain Admin Acct(s)								
	Local svr Admin Acct(s)								
	All users	Check the checkbox on all AD accts to chg pwd							
		Enforce strong password policy, if not already							
	Service Accts	Change pwd and standardize service accounts							
	Services	Change pwd on service startup like BE, SQL							
	Admin email addresses	Change any external email addresses sent to user							
5) Testing									
	Test logins								
	Test Email								
	Test core apps								
6) Physical Security									
	Change entry codes								
	Retrieve all keys								
	Retrieve all fobs								

* Add rows as needed for multiple entries; add new sections for multiple sites

[Client] - System Administrator Lockout Policy and Procedure

Policy

It is the policy of [Client] IT department to disable access and change system passwords whenever an IT administrator with elevated privileges leaves the company.

Procedure

This procedure is to be used whenever a domain administrator leaves [Client]. A domain administrator is defined as someone having access to all major IT systems and passwords. Any change in Cal Net IT personnel or [Client] IT management would be subject to this policy and procedure. The list of steps below are technical in nature and are not meant to be a comprehensive list of tasks for separation of an employee. They are only tasks required to ensure the network is secured.

Step 1 – Disable the user’s network and physical access

- Disable user account
- Change domain administrator password
- Revoke remote access rights to network
- Acquire/disable RSA tokens and access fobs belonging to the individual
- Inform staff that this person’s network rights have been revoked and are no longer with the company.

Step 2 – Change system passwords at main site and remote sites using checklist with system location, administrator account and passwords.

- Change firewall passwords
- Change SSL VPN password
- Change Anti-Spam password
- Change domain and SSL cert management passwords (Network Solutions, Thawte)
- Change passwords on any system account having remote access
- Change security system password
- Change video surveillance system password
- Change remove HVAC system management account password
- Change phone system management passwords
- Changing the following will interrupt business and require downtime -

- Change service account passwords (Any account that runs a service on any server having account login privileges)
- Change the VPN Client passphrase

Step 3 – Test all systems after changes are made using checklist

- Phone system
- FTP Server and website
- D.R. Site Systems
 - DFS Replication
 - Exchange replication
- Outlook, OWA and Activesync
- Anti-spam Appliance
- Fax Server
- E-Mail archiving solution
- Operational Systems (Video, HVAC, Security System)
- RSA tokens
- SSL VPN & VPN client
- Wireless access on LAN
- Document Management Systems
- Anti-Virus Systems
- Mobile computing Systems
- Backup Systems
- VPN tunnel clients

Step 4 – Communicate change to 3rd parties

- Inform each vendor having a relationship with the individual separated from the company that the employee is no longer with the company or Cal Net for support reasons
- Inform remote users of Sonicwall Global VPN client that the passphrase changed