



Lieberman Software

Complying With NERC/FERC Regulatory Standards

The North American Electric Reliability Corporation (NERC) is a self-regulatory body charged with ensuring that organizations delivering electricity to the North American electrical grid are identifying and protecting critical cyber assets. The Federal Energy Regulatory Commission (FERC) is the organization charged with overseeing the transmission of electricity, natural gas, and oil, but it gives NERC the responsibility for maintaining Critical Infrastructure Protection (CIP) standards in the electric industry.

To comply with NERC/FERC data security requirements, entities must establish methods, processes, and procedures for protecting systems that are deemed critical cyber assets. The ability to document and audit all infrastructure protection measures must also be established. Failure to do so can result in fines of up to \$1 million per day, per violation.

THE LIEBERMAN SOFTWARE SOLUTION

Lieberman Software’s privileged password management and configuration management solutions allow organizations to maintain fully audited control over access to mission-critical systems across the cross-platform enterprise. The company’s Enterprise Random Password Manager, Random Password Manager, User Manager Pro Suite, and Service Account Manager products help secure, manage, and log the use of highly-sensitive information by controlling access to privileged and shared accounts, and by identifying and remediating security threats.

Specifically, Lieberman Software helps organizations meet the following NERC/FERC account management, vulnerability assessment, and documentation mandates:

NERC/FERC OBJECTIVE	LIEBERMAN SOFTWARE SOLUTION
Manage the use of administrator, shared, and other generic account privileges	Automatically and frequently generate unique privileged passwords for every account in the enterprise
Ensure that individual and shared system accounts and authorized permissions are on need to know basis	Restrict ability to retrieve passwords to authorized personnel only; the scope of access is strictly limited based on individual “need to know”
Create audit trail of individual user account access activity	Produce audit-ready reports showing password changes and recoveries and program logons
Regularly review and verify appropriate user account access privileges	Verify occasionally that the local passwords assigned to each system are still functional
Identify individuals with access to shared accounts	Identify every account with administrative rights to every system in the network
Manage and secure shared accounts in the event of a personnel change	Prevent former IT employees from being able to gain administrative access
Establish policy for minimum length of passwords and special characters	Support password policy by creating passwords controlled for length, complexity and special characters