Recommendations

1 = Critical 2 = Essential 3 = Important

1 Review & Monitor Administrators' Logs

Logs of administrative activity should be reviewed for appropriateness by an individual other than the system administrator.

We do not recommend maintaining a generic "ADMIN" account. Instead, users should be granted administrative access so that audit logging can effectively identify activity based on the current user. Generic User IDs (i.e. "TEST") should be removed to reduce the likelihood of anonymous activity.

1 Restrict Third Party Vendor's Administrative Access

Your third party vendor should be required to request administrative privileged access on a case-by-case basis (i.e. user ID is inactivated when not in use) and should not retain it 24/7. Third party user ID's used should be identified as such, for example: "Admin-3." Access should be logged after it has been approved.

Third party vendor should inform you when a member of their team leaves or transfers jobs so that Graceland, Inc. can change the administrative password, and should be notified of any breach or information security event at the third party vendor.

1 Develop an End-user Information Security Policy

Develop a comprehensive information security policy for end-users such as employees, interns and vendors. The policy should include specific guidance (do's and don'ts) for employees and interns.

Example topics from a sample end-user policy include:

- Access Control
- Information Classification
- Physical & Environmental Security
- Acceptable Use of Assets
- Clear Desk/Screen
- Appropriate Transfer of Information
- Mobile Devices & Teleworking
- Restrictions on Software and Installation

A comprehensive, reviewed information security policy is a primary requirement of virtually every security standard and legislative regulation (i.e. HIPAA, PCI-DSS, etc.).