LANDAMERICA

Security Guidelines for System Administrators

LandAmerica Financial Group Inc.

Version 3.01 – November 22, 2002

LandAmerica Financial Group Inc.

Guidelines for All LandAmerica sites

Brief Summary

This document is intended to provide the system administrator with the standard for all office sites for LandAmerica Financial Group Inc. and our subsidiaries. This document applies to all platforms except Data General. It is not intended to cover the technical details of system or workstation configuration. The chapters of this document are:

I. User account administration

II. Server security

III. Desktop security

IV. Recurring security-related tasks

Chapter I . User Account Administration

User accounts are generated by analysts in the field using the naming convention currently in place: (2) letter state designation, (2) letter city designation, first initial of first name, first initial last name, and number identifier. In the case where there is more than one office in the same city, the offices should decide among themselves on the two-letter "city" designations.

Example: Tom Johnson at Las Vegas, Nevada is nvlvtj1.

Accounts must be created to log in to the Landam domain **only**, and given appropriate permissions to access objects within the resource domains. Landam accounts must be set up as follows:

- User accounts are setup with a forced password change upon first logging in to the network.
- The user has 90 days between forced password changes. The password length must be six characters or longer, except for system administrator passwords. Administrator passwords must be at least 10 characters long. It is recommended (but not required) that all users choose a password of at least ten (10) characters, which are a mix of upper- and lower-case letters, the special characters #$^_ and digits 0-9. Reuse of passwords is discouraged; the previous four (4) passwords are prevented from re-use. Passwords must not be set to "never expire."
- Particular care should be taken with administrator passwords and accounts as well as passwords for service accounts. These must not be shared, written down, or stored without encryption on any server, workstation, or diskette, except by using the following method:

Passwords are stored in a spreadsheet which is encrypte and password protected.
The spreadsheet has four columns:
Account, UserID, Password and Description

- Account is a general name for account (ex. NetBackup Service Account)
- UserID is the actual user account with domain (ex. landam\zzNetBackup)
- Password is the actual password
- Description is for more details (ex. Account used for NetBackup service on SVARIBUxx servers)
- The spreadsheet is ***encrypted with a password*** that includes more than 8 characters. Special characters, upper and lowercase, and numerals **must** be included.
- The spreadsheet is stored on an NT share that is protected by appropriate ACL for only administrators to access.

The spreadsheet is kept in alphabetic order by UserID

- Lockout is set to three attempts. Lockout status is removed after 15 minutes

- Resetting of a password to the last password used is prohibited.

- When an employee terminates or is terminated, the user login should be disabled as soon as the analyst is notified. The Help Desk should be notified in order to remove all other accounts. When the termination is not under positive circumstances, wherever possible contact the Help Desk ahead of time so that the accounts may be disabled simultaneous to the dismissal. The description field of a disabled account should be noted with the word DISABLED, as well as the date of disablement and the user ID of the administrator who disabled the account.

- It is acceptable to disable the account of a terminated employee, and then later rename the account login when a new employee is hired to do exactly the same job. That way, there is no doubt that the new employee has the exact same permissions as the previous one.

- Disabled accounts will be deleted after 90 days.

- Email accounts are hidden by Exchange administrators for 30 days and the User Account association is removed immediately. After 30 days, the email account is deleted.

Chapter II: Server Security

This section presents the general guidelines for maintaining security on an NT server. The sections of this chapter are:

A) Physical security of the server

B) File Security

C) Software security

D) Backups.

Section A – Physical Security

Servers, routers, and network connections should be placed in a location away from general access, preferably in a locked room. Access to this area should be restricted to the system administrator and his/her backup. The server should not be used as a workstation except by the system administrator, and then only for the purpose of server administration. Cable connections to the server should also be secured in order to reduce the risk of accidental or deliberate malicious damage to the physical equipment.

Where possible, the server location should be protected by a fire suppression system that is not water-based. At a very minimum, the server location should have a fire extinguisher within 50 feet of the server. This extinguisher must be capable of extinguishing class “C” (electrical) fires. It can be a multi-purpose fire extinguisher such as one rated for class “A” and class “C” fires, so that it can also be used to extinguish blazes from paper or cloth. The administrator should be aware, however, that such an extinguisher does not afford any fire suppression after normal working hours.

Originals of server software should not be stored in the server room. Ideally, they should be stored in an off-site location along with backup tapes. It is permissible to make backup copies of the software originals and store the copies near the equipment.

Section B – File Security

Access to files should be restricted to those who have a legitimate business need for that information. Administrators should be careful that inherited rights and permissions do not expose confidential data.

This is especially critical where the file contains non-public personal information about customers (for example, social security number, credit reports, and information of that nature). New privacy laws (Gramm-Leach-Bliley Act) require that such data on customers be handled in a secure manner.

Administrators should periodically review the server for the existence of files that are not business-related. Particular attention should be paid to photo, movie, and music files. The system administrator should report, in writing, to the office manager any such files that are found on the server. The office manager should determine if the files are business-related and request the removal of any which are not related to the conduct of LandAmerica business.

Section C – Software Security

Only software that is licensed to LandAmerica Financial Group is permitted to be loaded on LandAmerica servers. Users are not permitted to install any software on servers.

As system administrator, you should periodically inventory the server. When unauthorized software is found, the office manager should be informed in writing of its existence. The office manager should determine the legitimacy of the software, and either order its removal or send a photocopy of the license to the Information Security Office.

Operating system patches deemed “critical” by Microsoft or LandAmerica LAN Management must be installed within 21 days of their distribution from LAN Management.

It is especially important that sensitive system utilities be protected from unauthorized use. Access rights should be set up so that only the administration group has rights to sensitive areas such as the registration database, Server Manager, and other management utilities. Event logs, audit logs, and other security features must never be accessible by end users.

Section D – Backups

Backup domain controllers (BDCs) and other servers that contain application software, data files, or backup data from workstations, or which are used for anything other than a BDC must be backed up on a regularly scheduled basis using the written backup procedures for production servers.

The system administrator is responsible for implementing a tested and auditable process for backup and restoration of any non-production server. Such procedures are critical for recovery from hardware failures as well as physical disasters.

Wherever possible, backup procedures should not require any intervention by the system administrator. Backup and restoration procedures must be documented in writing, and must be tested at least annually. The results of testing these procedures must also be documented in writing, and a copy sent to the regional Technology Resources director as well as the Corporate Information Security Officer on an annual basis.

Backup media should be stored off-site so that in case of a physical disaster such as fire, flood, tornado, or earthquake, the backup media is not destroyed along with the physical equipment. In those areas where there are multiple company offices reasonably close to each other, offices can work together to store each other’s backups.

Chapter III: Desktop Security

This chapter addresses the security of the standard end-user workstation. These guidelines are intended to mitigate the risk associated with use of a workstation.

Workstations must be secured when the user is away from the desk for any period over 15 minutes, including overnight. The user may secure the workstation in one of the following ways:

- ❑ Locking the workstation by using Ctrl-Alt-Del

- ❑ Using a password protected screen saver with a time limit of no more than 15 minutes. In this case, the password must meet LandAmerica password standards.

- ❑ Logging out.

Anti-virus software must be installed and active on each workstation. Virus definition files may be no more than 3 days older than the most current definitions available from the software vendor. It is preferable that the latest version of the standard corporate anti-virus software be installed on the workstation so that new virus definitions may be "pushed" to the desktop. (See http://symantec.landam.com for more info on Anti-Virus)

One potential entry point for unauthorized access to LandAmerica systems is the existence of desktop modems. Most of the time, there should be no need for an individual workstation to use a modem. When modems are needed to communicate with banks or other business partners, it is preferred that a stand-alone PC (not network connected) be used for this purpose. Where a stand-alone system is not possible, the modem must be set so that "Auto-answer" is disabled.

Chapter IV: Recurring Security-related tasks

In order to maintain an efficient, secure environment, there are some tasks that need to be done on a regular basis. Timely completion of these tasks will help to assure that systems for which you are responsible are in compliance with LandAmerica's computer use policies. These tasks are:

Weekly

- □ Logins of all terminated employees have been disabled (if the System Administrator has been notified), and the Helpdesk has been notified of the termination.

- □ Servers have been backed up, and the backup media stored off-site

Quarterly

- □ File permissions verified and corrected as necessary. This is especially important when an employee has changed job responsibilities.

- □ Verify that all critical operating system patches distributed by LandAmerica LAN Management have been installed.

- □ Service accounts must be reviewed and passwords changed to comply with the 90 day standard.

Semi-Annually

- □ Workstations and servers scanned for unlicensed software. Unlicensed software reported to office manager and CISO. SMS reports may be used for this requirement.

- □ Servers and workstations scanned for non-business related media files (photos, music, and movies) and files reported to office manager and Corporate Information Security Officer (CISO).

Annually

- □ Written procedures for backup and recovery tested.

- □ Results of backup and recovery testing documented

- □ Test results reported to regional IS director and CISO

Ad Hoc (whenever you visit an office)

- □ Users are not writing passwords down; Verify by walking through work area looking for post-it notes, notes on corkboards, containing passwords.

- □ Workstations unattended for periods exceeding 15 minutes have been secured using one of the methods described in Chapter III.