INTEGRATED™ LENDING TECHNOLOGIES

# Statement Regarding Security, Controls & Procedures

## INTRODUCTION

For the convenience of its current and prospective clients, Integrated Lending Technologies, LLC (the "Company") has compiled the following summary of its technological infrastructure, its management objectives, the policies, procedures and internal controls put in place to achieve those objectives and a brief explanation of its history, organization and financial strength. Those needing more detailed information may contact Company management.

## SYSTEM RELIABILITY

Integrated Lending Technologies, LLC (the "Company") is committed to providing access and operation 24 hours a day, seven days a week without interruption for all its products, including DILLS™ and PILS® (the "Systems"). All reasonably practical steps have been taken to insure immediate and uninterrupted access by all authorized users of the Systems. Following are the major steps taken to achieve this goal:

**TABLE OF CONTENTS**


| | |
|---|---|
| System Reliability | 1 |
| Access Controls | 2 |
| Incident Response Procedures | 3 |
| System Upgrade Procedures | 5 |
| Data Management Procedures | 6 |
| Infrastructure | 9 |
| Computer Usage Policy | 12 |
| Financial Information | 15 |
| Audits | 15 |
| Network Layout Illustration | 17 |




PILS DILLS

1. The Primary Facility (see definition in Infrastructure below) provides bandwidth for the DILLS™ system on two GigE circuits and one OC48, with multiple backup links, providing direct peering to Level 3, UUNet, CenturyLink, and Cogent. The telecommunications network is delivered via Bellcore standards with secure conduit and separate entrance facilities.

2. All system data is backed up nightly at the Primary Facility in Salt Lake City via a snapshot on our storage array and replicated to a separate slave server residing on a physical host. A full system data restoration, if needed, would require about 25 minutes including database data and executable system code.

3. The primary location has raised floors, FM-200 fire suppression systems, multiple diesel backup generators, and extensive power conditioning and purifying. The building in which the facilities are housed conform to the highest standards for earthquake resistance. Monitoring software alerts all staff members of problems immediately.

4. DILLS™ runs on a Debian Linux platform. Disks are RAID 5, dual 3.0 GHz Zeon processors, 4GB memory. The database system is MySQL, the web server software is Apache and the programming language is PHP. Two mirred configurations run in parallel behind a load balancer to both improve performance as well as provide redundancy in case of hardware failure.

## ACCESS CONTROLS

The following procedures and controls for accessing the Systems are enforced by the Company:

**Administration Authority.** Access to all Systems is controlled by the President and each Vice President of the Company ("Management"). Management requires each agent, dealer and lender that has signed an access agreement (an "Authorized Organization") to assign at least one person within the respective

organization to have the responsibility to assign user names to each person having access to the Systems in that particular Authorized Organization. This person has the ability to inactivate any user in that Authorized Organization for violation of the access agreement or rules imposed by the Company or to require a password change. There is no limit on the number of persons within each organization that may have this level of administrative authority. Each organization is required to sign or accept the terms of an agency or access agreement in order to gain access to any of the Systems. These access agreements may be online agreements requiring digital acceptance by the user. For any person to access any System he/she must first enter into the appropriate field on the login page a user name and a password associated with that name. Not less than quarterly, Management reviews a master list of all user names and their associated levels of access (the "Access Policy Compliance Report") to assure compliance with this policy statement.

**Login Names.** Each user name must be associated with a natural person that is an employee or agent of each Authorized Organization. Management reviews the Access Policy Compliance Report on a regular basis (not less than quarterly) to insure that each user name is associated with the name of a natural person. User names and passwords are case sensitive.

**User Names.** A user name and unique password combination is required for each individual user to gain access to any System. Each user name may be any combination of alpha and numeric characters but must be at least four characters in length.

**Passwords.** Each user name must have a unique password assigned to it in order to gain access. That is, if a password is already in use when entered by a user for the first time, the user is required to enter a new password that is unique. The password must be at least six characters in length and must contain at least one alpha and one numeric character. Passwords must be changed every 90 days. When a user enters his/her password for the first time after the 90th day, the System will require him to change the password in order to gain access.

**Unauthorized Access.** If an incorrect password is entered by any user more than 5 times within the space of 15 minutes the user is provided a telephone number and e-mail address to contact for help. An e-mail is simultaneously generated to Management regarding the incident.

## INCIDENT RESPONSE PROCEDURES

The following procedures for detecting and responding to unauthorized or unusual attempted access to any System are enforced by the Company:

**Detection and Reporting.** The Company employs software that detects and records in the respective database all unsuccessful attempts to access any of its Systems more than five times within fifteen minutes from the same remote address which generates an e-mail alert to the President, the Vice President of Lender Relations and the Vice President of Technology of the Company containing the details of each such incident. The e-mail message contains the date and time of the attempts, the remote address from which the attempts were made, the user names and passwords used, the login name of the person associated with the user name (if such association exists) and the organization (agent, lender or dealer) associated with the login name (if such association exists).

**Response.** The three persons receiving the e-mail regarding each incident are responsible for determining the appropriate response to each such incident in the following order:

1. President of the Company
2. VP, Technology of the Company
3. VP, Lender Relations of the Company

That is, the President of the Company shall make the determination unless he is not able to respond for any reason, in which case the Vice President, Technology shall make the determination and so forth. Each person on the list shall inform the others on the list in advance if he/she will be unavailable for any reason. No person on the list shall take any action unless he/she has made

reasonable attempts to communicate regarding the matter with the person who appears from the e-mailed data to be making the login attempts.
If a determination is made by the responsible person that the attempt to log in is not being made by a person with appropriate authorization, the VP of Technology will be notified as soon as practicable and steps taken to disable the login for which the unauthorized attempts were made. Company management will make the decision if and when any such disabled login will be re-enabled or permitted to access any System. Company management will respond as it deems appropriate to each incident depending upon the nature and extent of each such event or pattern of events.

## SYSTEM UPGRADE PROCEDURES AND CONTROLS

The following procedures and controls for upgrading or altering DILLS™, PILS® or any of the equipment that supports or drives either such System will be enforced by the Company:

**System Changes.** The Vice President, Lender Relations and Vice President, Technology will have joint responsibility to maintain a Master Work List (the "List") on a secure, restricted access system available for review by all Management. The List will be divided into four parts:

1. Requests for change;
2. Projects in order of priority;
3. Projects under development; and
4. Completed projects.

All requests from any source for any change to the Systems will be considered by Management who will determine whether any such request will be added to the List. Periodically, Management (the President, the VP of Technology and the VP of Lender Relations) will meet to prioritize items on the List. Any project estimated to require more than a few hours to complete will be submitted to a developer, who may be a Company employee, for an estimate of time and cost before final priority placement on the List. Once prioritized, all projects will be described in appropriate detail before submission to a developer of Management's choice

for completion. The Vice President of Technology will monitor all projects under development to insure compliance with the order of priority and with the submitted specifications. Completed projects will remain on the List with a record of any changes made during development and testing and its final release date.

All development of System changes will be completed on a dedicated development server independent of the production server supporting the operation of the Systems. Once completed, all changes will be tested by Management, and one or more clients at Management's discretion, on the development server before installation and release on the production server. Version control software is used to control the source code and to provide code integrity. All development, testing, and production servers reside at the Primary Facility.

**Physical Security.** The production servers and related equipment necessary for the operation of the Company's production Systems are located in a third-party data center operated by ViaWest (www.viawest.com). The data center is located in Salt Lake City, Utah. The ViaWest data center has undergone an external SSAE16/SOC1 audit, and has issued the corresponding report, which contains all the physical and environmental controls and results of control testing.

## DATA MANAGEMENT PROCEDURES AND CONTROLS

The following procedures and controls for collecting, storing, managing and destroying information regarding loan applicants, lender participants and dealer or vendor participants in connection with its operation of the Systems will be enforced by the Company:

**Data Collection.** The Company will collect only the information regarding loan applicants ("Applicant Data") that is necessary to enable its lender clients, under their respective guidelines and procedures, to make decisions to extend credit and document loans, whether manually or through the use of the Systems' automated underwriting tools. This information will be collected only through the

online applications, from third party providers of online applications at dealerships or other vendors that are integrated with any System or through manual entry into a System by a participating lender, and from credit bureau reports.

The Company will collect information regarding loans made by participating lenders to loan applicants through its system as loans are funded by the participating lenders or as loans are terminated prior to normal expiration ("Loan Data").

Both Applicant Data and Loan Data are used by the Company to produce reports ("Reports") regarding system performance and to assist participating dealers and lenders to evaluate and manage their respective operations. Most of these reports are comprised of cumulative data only and will not contain individual Applicant Data or Loan Data relating to specific applicants or loans. Some of the Reports will contain applicant names and associated Applicant Data and Loan Data.

**Data Storage.** Applicant Data and Loan Data are stored on the Company's servers as collected. The servers are located in the Primary Facility in Salt Lake City. The Applicant Data and Loan Data are backed up to a secondary server at the end of each day. Some Reports may be printed by the Company and stored in filing cabinets in the Company's office.

**Access to Data.** All members and all employees of the Company with Manager or higher level of responsibility have access to all data through central administrative level passwords. Management will make all decisions regarding whether any additional employees of the Company will be granted access depending on the need for administrative or system development or maintenance purposes. All Company employees with Manager or higher level of responsibility will have access to the Company's filing cabinets. Upon termination of employment of any employee of the Company, such employee's access to all Systems and to the Company files will be immediately revoked.

Dealer or vendor participants will have access only to Applicant Data entered into DILLS™ or PILS® by the consumer applicant or by their own employees that have been granted access and to credit scores of individual applicants returned by the credit report of each participating lender to which the dealer or vendor submits an application. The dealer/vendor access will not include credit report information from a lender participant's credit report (except for each applicant's credit score returned by the lender's credit report on such applicant) unless the dealer or vendor is specifically granted access by a participating lender. A dealer will only have access to Reports relating to its own Applicant Data. Each dealer participant determines the level and extent of access by its own employees.

Lender participants will have access only to Applicant Data entered into DILLS™ or PILS® by their own employees that have been granted access, to Applicant Data received through such System from a dealer or vendor participant and to Loan Data relating to loans funded by such lender through the use of such System. A lender will only have access to Reports relating to its own Applicant Data and Loan Data. Each lender participant determines the level and extent of access by its own employees.

Agents will have access to Applicant Data, Loan Data and Reports relating to dealers and lenders in such agent's area of agency. Each agent determines the level and extent of access by its own employees.

**Destruction of Data.** All data in the Systems' databases will be stored on the Company's servers and backup servers for at least seven years from the date on which the Applicant Data is first entered into a System. After the expiration of the seventh year, such Applicant Data and all data relating to such Applicant Data may be permanently deleted at the discretion of Management.

The Company's filing cabinets will be inspected annually, and any printed Reports containing Applicant Data made by the Company more than 12 months prior to such inspection shall be destroyed by shredding.

## INFRASTRUCTURE

The Company hosts its Systems in a security-conscious environment to prevent unauthorized access to customer data and breach of system security. Numerous steps have been taken to ensure the security of the Systems.

1. The servers and related equipment necessary for the operation of the Company's web-based systems are located in a suburban Salt Lake City data center (the "Primary Facility") operated by ViaWest (www.viawest.com). Following is a brief description of the Primary Facility infrastructure and support:

    - Operates 19 UPS modules.
    - Maintains 2,400 UPS backup batteries.
    - Generates over 5,250 KW of power as needed.
    - Produces 1,460 tons of cooling capacity.
    - 94,000 square feet of raised floor capacity.
    - 1,706 ¼ cabinets.
    - Situated in a region with only 9 disasters since 1953, the lowest west of the Mississippi.
    - 24x7 onsite engineers.
    - 100% SLA for power, bandwidth, and network services availability.
    - 27 telecommunication carriers ensure a carrier-neutral position regarding network connectivity.
    - 87% first-call resolution.

2. All traffic passes through a firewall to a switch through the load balancer. The firewall functions as a router which also performs access control and VPN connectivity to create a secure DMZ. The firewall is required for the System to function, so when it is not in place, the System is inaccessible. Only one DMZ exists, and since the servers are located in a secure facility, no general-purpose machines are connected to this DMZ. All general-purpose computers are located outside the firewall/router in other physical office locations, making the infection of a server by a general-purpose machine with any virus impossible.

3. Servers are not permitted to access random servers on the Internet which is controlled by firewall policies. All System data transferred over the Internet is encrypted via 128-bit SSL certificates.

4. All servers are maintained with the latest security patches made available by the Debian Linux operating system. Additionally, the VP of Technology receives periodic security alerts from US-CERT and from Debian, which include information on potential vulnerabilities and their impact on the Systems.

The Systems have not had a security breach since the Company began operating in July 2001.

## COMPUTER USAGE POLICY

The following policy regarding the use of computer equipment owned by the Company or the use of its network, e-mail accounts, websites or systems is strictly enforced:

**Unacceptable Use.** The following activities are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of the Company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Company-owned resources. The lists below are by no means exhaustive, but provide a framework for including activities which are unacceptable.

**System and Network Activities.** The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of

"pirated" or other software products that are not appropriately licensed for use by the Company.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or the end user does not have an active license.

3. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. Management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing account passwords to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.
6. Using any Company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from the Company account.

8. Making statements about warranty, whether express or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of

which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forging routing information for malicious purposes.

10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job duties.

11. Circumventing user authentication or security of any host, network or account.

12. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

13. Using any program, script, or command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session via any means, locally or via the Internet/Intranet/Extranet.

14. Providing information about or lists of the Company employees to parties outside the Company without prior authorization from Management.

15. Accessing nonpublic private information regarding individual credit applicants stored in the DILLS™ database unless required for the performance of the user's duties or using any such information except for the purposes for which it was intended to be used by the applicant(s).

**E-mail and Communications Activities**

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material generally considered to be e-mail spam to

individuals who did not specifically request such material.

2. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use or forging of e-mail header information.

4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding chain letters, "Ponzi" or other pyramid schemes of any type.
6. Use of unsolicited e-mail originating from within the Company's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Company or connected via the Company's network.

7. Posting the same or similar non-business related messages to large numbers of Usenet newsgroups (newsgroup spam).

**Enforcement.** Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

## FINANCIAL INFORMATION

The Company or its predecessor company has been operating and managing DILLS™ since August of 2001. The Company now has lender and dealer users in many states and is expanding into new markets every month. Revenue growth exceeds 20 % annually. However, the Company remains closely held and does not make its financial information available. We can disclose, however, that the Company has no debt and is profitable.

## AUDITS

An audit of the Primary Facility was recently performed by Ernst & Young, LLP, in

accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16. A copy of the audit report is available upon request.

An audit of the Company was recently performed by Cadence Assurance LLC, in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16. A copy of the audit report is available upon request.

# ILT NETWORK LAYOUT