TeleDirect

| | | |
|---|---|---|
| **TeleDirect Call Centers<br>Information Security Management System** | Document #<br>**TD29** | Page<br>**1 of 1** |
| **ISMS Scope** | Effective Date<br>10/1/2016 | Version<br>3.0 |

TeleDirect Communications Inc. is committed to protecting all non-public information at our facility which is located at 4745 Chippendale Drive in Sacramento, California.

TeleDirect has established an Information Security Management System (ISMS) in accordance with the requirements of ISO standard ISO/IEC 27001:2013, implementing controls per Statement of Applicability dated 10/1/2016. The ISMS framework serves as TeleDirect's mechanism to appropriately identify, select, maintain, and improve information security controls that are critical to its clients and business. The Statement of Applicability version is v3.0

Boundaries of the ISMS that were included in scope were:

- Secure storage, transmission and replication of sensitive information
- Client support services
- Internal IT
- Human resources
- Physical and environmental access controls
- Incident management - "security incidents"

Boundaries of the ISMS that were excluded from scope were:

- Outsourced data center locations
- All other incidents not deemed security incidents

**DOCUMENT HISTORY LOG**

| STATUS | DOCUMENT REVISION | EFFECTIVE DATE | DESCRIPTION |
|---|---|---|---|
| Baseline | N/A | 10/1/2016 | Initial version of ISMS Scope. |

Owner: ISMS Manager

Document Approval: Celia Puff
Name/Title/Date: CELIA PUFF, CEO 10/1/2016

TeleDirect

| TeleDirect Call Centers<br>Information Security Management System | Document #<br>**TD30** | Page<br>**1 of 1** |
|---|---|---|
| **Information Security Policy** | Effective Date<br>10/1/2016 | Version<br>3.0 |

TeleDirect works with a variety of information critical to our ongoing success. To protect our clients, callers, employees and TeleDirect, we must ensure information integrity, confidentiality, and accessibility is maintained. Our ISMS objectives are established once the risks unique to our business are evaluated. Risks are evaluated by identifying the threats that present the most danger and our vulnerability to those threats, taking into account the value of the asset at risk. We measure our success controlling these risks through regular reviews and audits where we examine the logs and controls in place to detect security incidents.

Our objective is to have no security incidents that result in the loss of data confidentiality, accessibility or integrity each quarter. To measure this objective, we review our firewall logs, server reports and security incident reports during each audit. If our audit reveals a risk to our information security, continuity or compliance with our legal or contractual obligations an immediate risk assessment is done and corrective action taken.

The Information Security Policy is scheduled to be reviewed annually in conjunction with the annual Management Review meeting. This review is to ensure its continuing suitability, adequacy and effectiveness.

Definitions:
When TeleDirect refers to data accessibility, we mean that data is available on-demand to any authorized entity, whether a caller, client, or employee.

When TeleDirect refers to data confidentiality, we mean that data is not available to any unauthorized entity.

When TeleDirect refers to data integrity, we mean the safeguarding of the accuracy and completeness of data.

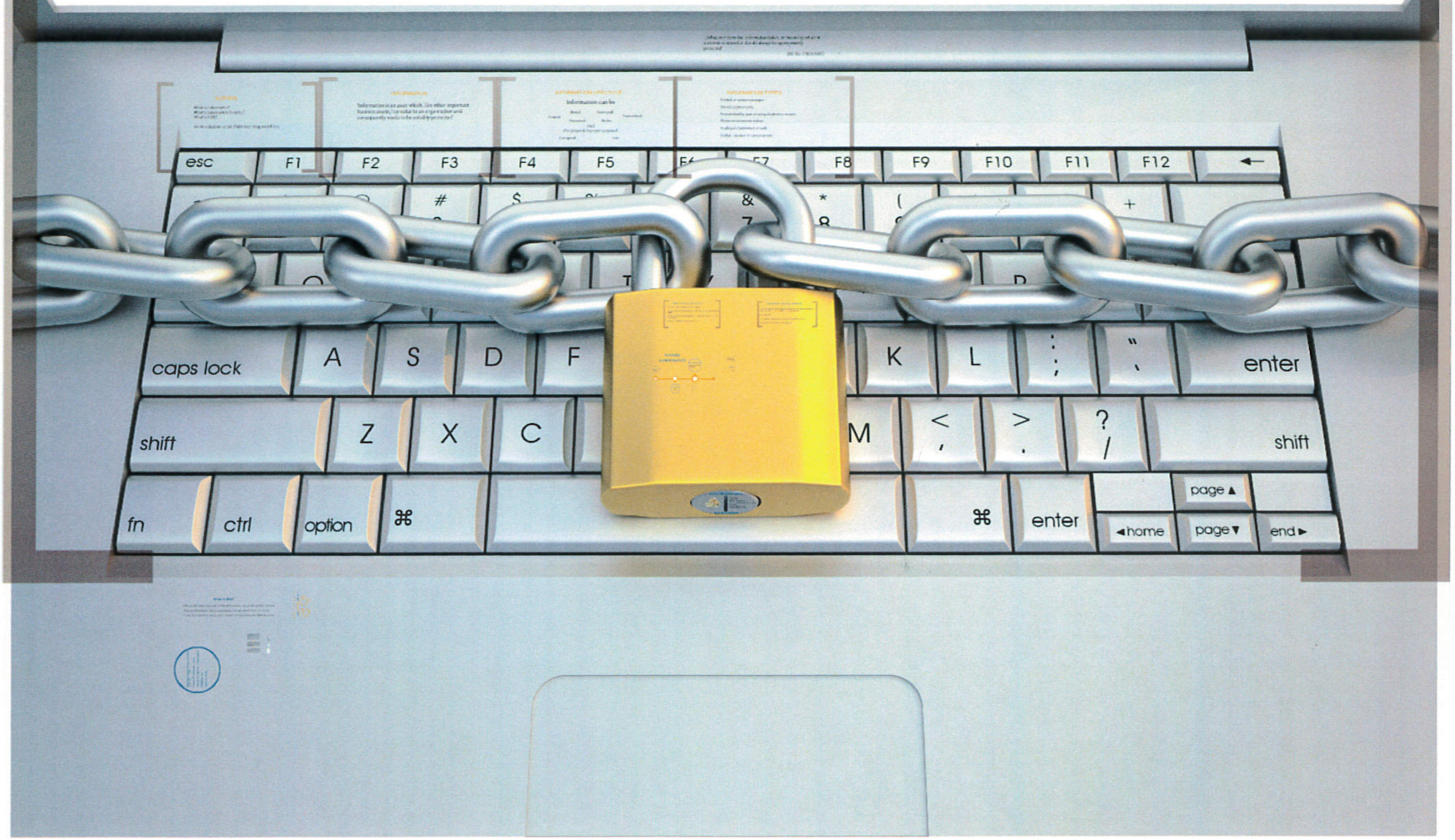
**DOCUMENT HISTORY LOG**

| STATUS | DOCUMENT REVISION | EFFECTIVE DATE | DESCRIPTION |
|---|---|---|---|
| Baseline | N/A | 10/1/2016 | Initial version Information Security Policy |

Owner: ISMS Manager

Document Approval: 
Name/Title/Date: CELIA PUFF, CEO, 10/1/2016

# Welcome To
# TeleDirect's ISMS Awareness Training
# ISO 27001:2013



# What Is Information Security?

- The quality or state of being secure to be free from danger
- Security is achieved using several strategies simultaneously or used in combination with one another
- Security is recognized as essential to protect vital processes and the systems that provide those processes
- Security is not something you buy, it is something you do

# Information Security…continued

The architecture where an integrated combination of systems and solutions, software, alarms, and vulnerability scans work together

Monitored 24x7

Having People, Processes, Technology, policies and procedures

Security is for PPT and not only for  devices

# ISO 27002:2005 defines Information Security as the preservation of:

**Confidentiality**

Ensuring that information is accessible only to those authorized to have access

**Integrity**

Safeguarding the accuracy and completeness of information and processing methods

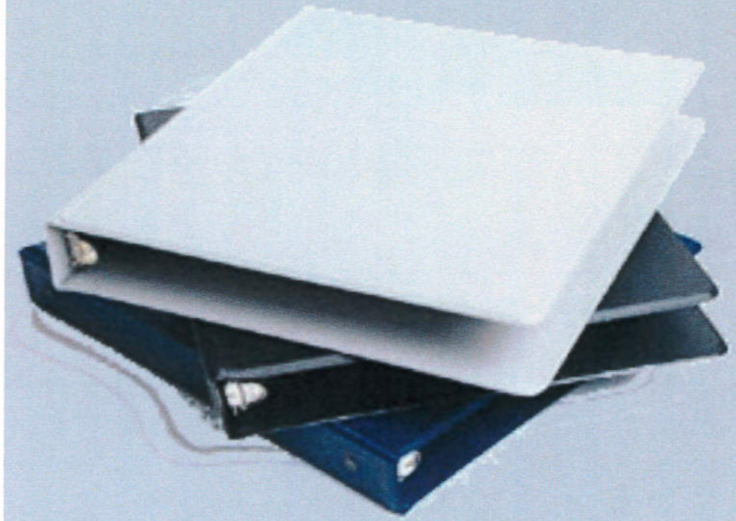
**Availability**

Ensuring that authorized users have access to information and associated assets when required

# Features of ISO 27001

- Plan, Do, Check, Act (PDCA) Process Model
- Process Based Approach
- Stress on Continual Process Improvements
- Scope covers Information Security not only IT Security
- Covers People, Process and Technology
- 5600 plus organizations worldwide have been certified
- 11 Domains, 39 Control objectives, 133 controls

# Information Security Policy



TeleDirect's Information Security Policy is:

- Approved by Top Management
- Released on the Internal Dashboard
- Placed on the back of your ID badge

# Access Control - Physical

👍

Follow Security Procedures
Wear Identity Cards and Badges
Ask unauthorized visitor his/her credentials
Unattended visitors in Reception and Conference Room only

👎

Bring visitors in operations area without prior permission
Bring hazardous and combustible material in secure area
Practice “Piggybacking”
Bring and use pen drives, zip drives, ipods, other storage devices unless and otherwise authorized to do so

# Security Incidents

Report Security Incidents (IT and Non-IT) to
Supervisor and or ISMS Team through
Face to Face
Dashboard Ops Center (single recipient)

e.g.:
IT Incidents: Mail Spamming, Virus attack, Hacking, etc.
Non-IT Incidents: Unsupervised visitor movement, Information leakage, Bringing unauthorized Media

Do not discuss security incidents with any one outside TeleDirect
Do not attempt to interfere with, obstruct or prevent anyone from reporting incidents