INSIDESALES.COM

Information Security Policy

Policy owner: Dan Wadsworth
Policy review frequency: Annual
Last Author: Dan Wadsworth
Last Revised Date: 12/14/2018
Version #: 1.15

Executive Summary

InsideSales.com proactively employs policies and procedures to ensure secure business practices. An internal oversight committee manages security policy generally, and oversees compliance for company operations and technologies.

InsideSales.com uses industry-standard practices and guidelines as the basis for policies, including:

NIST 800

Trust Services Principles and Criteria (SOC2)

ISO27001:2013 / 27002:2013

Payment Card Industry Data Security Standard (PCI-DSS)

Applicable government statutes regulating personal information such as HIPAA, the Massachusetts Standards for the Protection of Personal Information, and California's data breach notification law.

Open Web Application Security Project (OWASP) standards

Certifications

SSAE16 SOC2 Type II for Security, Availability, and Confidentiality Trust Principles

Definitions

Corporate Entity

For brevity, references to InsideSales.com may be shortened in this text using "InsideSales," or "IS.com."

References to actions performed by InsideSales.com employees will regularly use the joint first-person "we" in this document. In these cases, such references ("we," "us," "our," and "ours") should be assumed to refer to an authorized employee or employees within InsideSales.com, Inc.

Unless otherwise stated, references to "the committee" or "security committee" refer to IS.com's internally appointed security steering committee, as defined in this document.

Product

In some cases, we use "InsideSales.com" and its shortened derivatives to refer to the corporate legal entity, InsideSales.com, Inc.; in other cases, we use it to refer to the actual service platform and software we provide. Contextually the usage should be apparent.

Throughout this document we may refer to the InsideSales.com computing platform and its attendant applications generally in the following terms: "software," "system(s)," "platform," "application(s)," "suite," "tools," or some combination of these terms (e.g., "application suite").

General references to telephony-specific areas of the platform may be referred to as "the dialer" or simply "dialer," "dialer system," "telephony platform," "telephony suite," or some combination of these terms.

References to a specific application within the platform will be referred to by their proper name, such as the PowerDialer™.

References to the InsideSales.com PowerDialer™ for Salesforce product may regularly be abbreviated using the acronym "PDSF."

References to the InsideSales.com Lead Management Platform product will regularly be abbreviated as "LMP," "IS.com LMP," or "IS.LMP."

Other

As an authorized Salesforce partner, we regularly refer to the Salesforce CRM, and the salesforce.com corporate entity. We follow, as much as possible, salesforce.com's recommended naming conventions for the company and its products and services, where "salesforce.com" is the correct reference to the actual corporate entity, and "Salesforce," "Force.com," and / or "Salesforce CRM" refer to the sales automation software it provides.

Any registered trademarks, service marks, copyrights, or other intellectual property related to salesforce.com and its products are property of salesforce.com, Inc.

In most cases we make no distinction between security items for IS.com LMP products and products built for the Salesforce CRM, as the core infrastructure and code base is nearly identical between them. In cases where the distinction is relevant, we will define which platform is specifically affected, using the appropriate "LMP" or "Salesforce" platform qualifier.

Scope

This policy defines common security requirements for all Insidesales.com personnel and systems that create, maintain, store, access, process or transmit information. This policy covers the Insidesales.com network system which are comprised of various hardware, software, communication equipment and other devices designed to assist Insidesales.com in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Insidesales.com domain, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by Insidesales.com at its office location or at remote locales.

Information Security Program

The ISDC Information Security Program consists of standards, guidelines, policies, and procedures for the protection of ISDC information and assets. The content of this program must be followed by all employees, contractors, part-time and temporary workers, and those employed by others to perform work on ISDC premises or who have been granted access to company information or systems.

The term, “Information” as used in this policy includes but is not limited to, electronic, printed, faxed, processed, transmitted, or discussed information.

Overview

Information is an essential ISDC asset, and is vitally important to ISDC business operations and long-term viability. ISDC continuously strives to ensure that its information assets are protected in a manner that is reasonable, prudent and that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

The Information Security Program provides the framework to ensure the confidentiality, integrity, and availability of ISDC data through policies designed to assess, identify, prioritize, and manage organizational risk. Management activities support organizational objectives for mitigating these risks along with metrics created and used to gauge improvements in risk mitigation.

The Information Security Program has adopted an asset management approach to Information Security that requires the identification, assessment, and appropriate mitigation of risk that can adversely influence ISDC information assets.

The Information Security Program content will be updated as required by the Information Security Officer (ISO) or Chief Information Security Officer and approved annually by the InsideSales.com executive management.

1. Information Security Governance Policy

Purpose

Information Security Governance establishes the necessary framework to govern all aspects of Information Security. The primary objective of governance is to enable consistency in identifying, monitoring, and resolving information security related risks within the organization.

Scope

The scope of governance encompasses Information Security tools and technology, management of Information Security processes & policies, Information Security risk assessment, adherence to standards, oversight for solutions developed & implemented and technology vendor management/oversight.

Information Security Steering Committee

The Information Security Steering Committee consists of the following members:

- Chief Financial Officer, VP of Technology, Chief Information Security Officer, Director of Operations, Information Security Architect, VP of Development, IT Enterprise Architecture, and other specialists as required.

The Information Security Steering committee charter includes the following functions:

- Assess corporate-wide security policy and ensure that business requirements are reflected in the security policy.
- Assess requests for policy exceptions.
- Evaluate and approve corporate-wide security solutions.
- Act as custodian and governance body of the enterprise security program.
- Assess and approve any outsourcing of security services.
- Represent the organization in all corporate security matters.
- Act as custodian of corporate-wide strategic security processes (e.g., role analysis, data classification).
- Coordinate and validate any external, security-related corporate communication plans and activities (e.g., in the event of a high-profile, publicized security breach).
- Track major business IT solutions and identify opportunities to leverage security solutions.
- Evaluate the effectiveness of security monitoring solutions.
- Evaluate the impact of any new Regulations, bulletins, or security related communications from Regulators, clients, or Industry sources.
- Establish action plans for security strategies.
- Updates are provided to the ITSC by the Chief Information Security Officer and other members of the IT management team.

Information Protection Roles

Owners, Custodians, and Users are responsible for the security of ISDC data. ISDC owns all corporate data and applications; however, primary responsibility for the data falls to the business unit manager

who has requested the creation of the data or is designated as the primary user of the information. Multiple business units may have joint ownership of information when it is utilized across departments.

Administrator and Owner

The Administrator is the information owner. They are responsible for defining the classification of the data, authorizing access to the data, and assigning control requirements to the custodians for the data.

The owner must understand how the data is generated, stored, and processed before they can work with the custodian to determine the administration of the access controls.

Custodian

The Custodian is responsible for storing and processing the information. They are also responsible for administering access controls that have been specified by the owner.

User

The User is someone who has been authorized to read, enter, change or duplicate information. They have the responsibility to use this information only for the purpose intended by the data owner. The User is charged with complying with all access controls and maintaining the confidentiality of the data.

Chief Information Security Officer

The Chief Information Security Officer is responsible for the maintenance and coordination of the Information Security Program. They have the authority and responsibility to create and enforce policies to protect the confidentiality, integrity, and availability of ISDC data.

Information Security Policy Approvals

New policies relating to the Information Security Program will be reviewed by the ISO and approved by the Information Security Committee. Upon approval, the ISDC IT security team will adopt the policy.

2. Security Awareness and Training Policy

Purpose

A strong Information Security program cannot be implemented without training users on security policy, procedures, and techniques, including management, operational, and technical controls. Those who manage the IT infrastructure must have the necessary skills to carry out their assigned duties effectively. Failure to provide security training puts an enterprise at great risk because security of resources is as much a human issue as it is a technology issue.

Scope

Everyone has a role to play in the success of a security awareness and training program. Directors, Executive Officers, VPs, and business unit managers have key responsibilities to ensure that an effective program is established company wide. The scope and content of the program must be tied to existing security program directives and established security policy.

The security training function will be fully decentralized meaning only policy development resides with Information Security and all other responsibilities are delegated to individual business units. This policy will be reviewed annually by the Chief Information Security Officer.

Policy

Business unit owners are to ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Each employee must attend an employee orientation and an annual training refresher. Such training shall ensure that employees are versed in the rules of the system, provided the latest security updates, and apprise them about technical assistance available to them. As part of an application security plan, before allowing individuals access to the application, business unit owners must ensure that all individuals receive specialized training focused on their responsibilities and the application rules.

Additionally, ISDC assigns the business unit owners with the responsibility to ensure that the unit has trained personnel sufficiently to assist the business unit in complying with these requirements and related policies, procedures, standards, and guidelines. The security awareness training will be used to inform personnel, including contractors and other users of information systems.

Related Procedures

The strategy adopted by ISDC is to ensure that the security policies are known throughout the corporation and to establish the foundation of a corporate wide plan, and then progress to the awareness of Federal guidelines and regulations. The scope of the awareness training will be limited and focused on these areas.

Policies and procedures are made available to all employees on the corporate intranet site.

A significant number of topics can be mentioned and briefly discussed in any awareness briefing. Topics may include:

- Password usage and management
- Protection from viruses, worms, Trojan horses, and other malicious code
- Policy – implications of noncompliance

- Unknown e-mail/attachments
- Web usage – allowed versus prohibited; monitoring of user activity
- Social engineering
- Incident response – contact whom? “What do I do?”
- Handheld device security issues – address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information
- Laptop security while on travel – address both physical and information security issues
- Personally owned systems and software at work
- Access control issues – address least privilege and separation of duties

Changes and Compliance

It will be necessary to ensure that the program, as structured, continues to be updated as new technology and associated security issues emerge. Training needs will shift as new skills and capabilities become necessary to respond to new architectural and technology changes. Employee orientation will be conducted for each staff member as well as an annual refresher course that each employee is required to attend.

The Chief Information Security Officer will present on a current event topic annually and review all corporate Information Security policies to ensure nothing should be added to either the refresher or the orientation presentations.

When changes occur that need to be addressed from an IT security standpoint, the business unit can do the following:

- Contact the Chief Information Security Officer to discuss a briefing
- Contact HR to see about incorporating it into New Hire orientation
- Contact the Chief Information Security Officer to inform her/him regarding the briefing you will be providing for your business unit.

3. Asset Protection Policy

Purpose

The *Asset Protection Policy* defines the ISDC objectives to establish specific policies to protect the confidentiality, integrity, and availability of Company information assets. Company information assets are defined in the Data Classification Policy.

The Asset Protection Program conforms with the ISDC asset management approach to Information Security that requires the identification, assessment, and appropriate mitigation of risk that can adversely influence ISDC information assets. This program incorporates industry best practices, Gramm-Leach-Bliley Act safeguards, NIST 800 series standards and ISO 17799 recommendations.

Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company premises or who have been granted access to Company information or systems, are covered by this policy and must comply with associated policies and guidelines.

Policy

This policy identifies the different paths ISDC data may be accessed through. The identification of those elements and the policies which control them has been identified within this policy. This policy defines objectives for establishing specific standards for protecting the confidentiality, integrity, and availability of ISDC information assets.

Related Procedures

- Authorization for access to information assets will be based on the classification of the information and defined to provide only the minimum level of access required to meet an approved business need, or to perform prescribed job responsibilities. Proper identification and authentication are required. Specific instructions and requirements to control access to information assets are provided in the Access Control Policy.
- Authorization for remote access to information assets will be provided only to meet an approved business need, or to perform prescribed job responsibilities. Specific instructions and requirements for accessing information assets remotely are provided in the Remote Access Policy.
- Information assets must be protected with physical access control of areas containing information assets or processing activities. Specific instructions and requirements for physical access to information assets are provided in the Physical Access Policy.
- Encryption must be used to protect Restricted and Confidential information assets that will be transmitted over non-secure or public networks. Storing Restricted and Confidential information assets must be achieved with similar approved encryption methods. Only Company approved encryption algorithms and products can be used to protect Restricted and Confidential information.
- Information assets are created and maintained with appropriate controls to ensure the information is correct, auditable, and reproducible. Specific instructions and requirements for protecting the integrity of information assets are provided in the Data Classification policy.

- ISDC has established appropriate controls to ensure information assets are consistently available to conduct business. Business continuity planning, to effectively back up, replicate, and recover information assets, as necessary, must be established.
- Information assets are protected from destructive software elements such as viruses and malicious code that can impair normal operations. Company-approved virus detection programs are installed, enabled, and updated on all systems susceptible to viruses and malicious code. Specific instructions and requirements for protecting information assets from viruses and malicious code are provided in the Anti-Virus Policy.
- Auditing is activated to record relevant security events. The audit logs are securely maintained for a reasonable period of time.

Responsibilities

The Information Security Officer (ISO) is the approval authority for the Asset Protection Policy.

The Chief Information Security Officer is responsible to develop, implement, and maintain the Asset Protection Policy, and associated standards and guidelines.

Individuals, groups, or organizations, identified in the scope of this policy are accountable for one, or more of the following levels of responsibility when using Company information assets:

- Owners are Business unit managers who have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the ISO will make the designation.
- Owners are responsible to:
    - Define procedures that are consistent with the Asset Protection Policy and associated standards
    - Ensure the confidentiality, integrity, and availability of information assets
    - Authorize access to those who have an approved business need for the information
    - Ensure the revocation of access for those who no longer have a business need for the information
- Custodians are the network administrators who manage, process, or store information assets. Custodians are responsible to:
    - Provide a secure processing environment that protects the confidentiality, integrity, and availability of information
    - Administer access to information as authorized by the Owner
    - Implement procedural safeguards and cost-effective controls
- Users are the individuals, groups, or organizations authorized by the Owner to access the information assets. Users are responsible to:
    - Use the information only for its intended purposes
    - Maintain the confidentiality, integrity, and availability of information accessed, consistent with the Owner's approved safeguards while under the User's control.

Policy Enforcement and Exception Handling

Failure to comply with the Asset Protection Policy and associated standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions may be taken for violations of applicable regulations and laws. Requests for exceptions to the Asset Protection Policy should be submitted to the ISO. Exceptions shall be permitted only on receipt of written approval from the ISO.

4. Technology Acceptable Use Policy

Purpose

The use of technology resources, including email, voice mail, and Internet access, to communicate business-related data, has become critical to our business. Although these resources promise faster and better communications, they also raise significant issues concerning the security and control of information, especially in connection with confidential and proprietary business information. This policy accordingly serves to define the parameters of appropriate and professional use of ISDC technology resources. For purposes of this policy, the term "ISDC" includes InsideSales.com and all of its subsidiaries.

Scope

This policy applies to the following.

1. All ISDC employees and all other persons authorized to use Technology Resources (referred to, collectively, as Users)
2. All ISDC-provided technology resources, including but not limited to computers (e.g., desktop and portable computers, servers, networks, printers, software and data storage media), e-mail, voice-mail, facsimile machines, photocopiers, and Internet use (referred to, collectively, Technology Resources)
3. All data created, entered, received, stored, accessed, viewed or transmitted by the use of Technology Resources. This includes, but is not limited to, all confidential and proprietary information that belongs to ISDC and the disclosure of which could harm ISDC or its employees and provide an unfair advantage to ISDC competitors (e.g., information in any way related to ISDC intellectual property, research and development, personnel, recruiting, finances, profits and business plans).

Detail

All users of technology resources must comply with the following provisions:

1. **Proper Use.** Other than occasional personal use of voice-mail, e-mail and Internet access, Technology Resources may be used only for legitimate business-related communications. Occasional personal use means infrequent, incidental use that is professional, in good taste and does not interfere with ISDC business, the performance of the User's duties or the availability of Technology Resources. Technology Resources may not be used to run or solicit outside business ventures. All use of Technology Resources, including all personal use, is subject to this policy.
2. **Data Ownership.** All data created, entered, received, stored, accessed, viewed or transmitted via Technology Resources are ISDC property. ISDC has a perpetual, royalty-free, irrevocable, non-exclusive right and license to use, reproduce, modify, adapt, publish, distribute and incorporate all such data. Business-related data may not be used for any purpose unrelated to ISDC business. It may also not be sold, transmitted, conveyed or communicated, in any way, to anyone outside of ISDC without senior management's express authorization.
3. **No Privacy.** Users have no expectation of privacy in connection with the use of Technology Resources, including the creation, entry, receipt, storage, access, viewing or transmission of data.
4. **Monitoring.** As with all other ISDC property, ISDC may search, monitor, inspect, intercept, review, access and/or disclose any Technology Resources. This includes any data created, entered, received, stored, viewed, accessed or transmitted via those resources for any reason,

at any time. This may be done without advance notice of persons designated by or acting at the direction of the ISDC Chief Information Officer, or as may be required by law or as necessary for or incidental to auditing, security and investigative activities, and to ensure effective technology resource administration and policy compliance. For example, authorized persons may inspect Technology Resources to investigate theft, the unauthorized disclosure of confidential and proprietary information, misuse, and to assess Internet use. ISDC will attempt to ensure that monitoring and inspections are conducted professionally. In this regard, no employee (including officers, managers and supervisors) may search, inspect, intercept, review, access or disclose any data without the authorization of the ISDC Chief Information Officer or persons designated by them or acting at their direction.

5. **No Harassment.** Users are absolutely forbidden from using Technology Resources in any way that may be construed to violate the ISDC harassment-free workplace policy. This prohibition includes sexually explicit or offensive images, messages, cartoons, jokes, ethnic or religious slurs, racial epithets or any other statement or image that might be construed as harassment or disparagement on the basis of race, color, religion, sex, national origin, age, disability, sexual orientation, or any other status protected by law. Users are required to take all reasonable steps to avoid and eliminate receipt of any potentially offensive material. Prohibited conduct includes sending email messages to someone who has requested that the User not do so.
6. **Unlawful Use.** Technology Resources may not be used to intentionally or unintentionally violate any local, state, federal or international civil or criminal law, including copyright and patent laws. Users may not upload, post, e-mail or otherwise transmit any unlawful materials or any data that is threatening, abusive, malicious, torturous, defamatory, libelous, vulgar, obscene, or invasive of another's privacy.
7. **Proprietary Rights.** Technology Resources may not be used to violate proprietary rights, including copyright, trademark, trade secrets, right of publicity or any other intellectual property rights. For example, unless consistent with all applicable licenses and approved by the ISDC Chief Information Officer (or designee), Users may not post or download any data (including software) protected by copyright or patent law. Likewise, Users may load only licensed software from the Internet or other source onto a ISDC-provided workstation or laptop, provided that use of the software is consistent with the license and the original software license remains at the appropriate ISDC office so that ISDC may conduct accurate audits (and respond to external audits).
8. **Passwords and Security.** All passwords and security used in connection with Technology Resources, including voice mail access codes, are ISDC property and must be made available to ISDC. Users must understand that their use of passwords will not preclude access, monitoring, inspection, interception, review, or disclosure by authorized ISDC personnel. ISDC may also, unilaterally assign or change passwords and personal codes. The security of Technology Resources is every User's responsibility.
9. **Viruses, Downloads from the Internet and Internal Email.** Users may not upload, post, e-mail or otherwise transmit any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware or telecommunications equipment. Users who download data from the internet must do so only to their local C: drive and not the network (unless the User's only access is via a network computer that only has network drives available). Users must not download or open any files from an unknown origin, including e-mail attachments. For security and performance purposes, all e-mail attachments must be less than four (4) megabytes. Users must not run remote control application software that can make the User's computer accessible to the

Internet (including, but not limited to, PC Anywhere, Windows file and printer sharing, and FTP servers or personal web servers).

10. **Hardware.** The ISDC Information Technology (IT) Department establishes the standards for computer hardware acquisitions, including the standards related to the lease, purchase or rental of hardware; the brand of hardware and peripheral equipment; maintenance contracts; and service vendors. Users may not remove ISDC hardware or ISDC data stored in data storage devices, from the premises without permission. No personal computer hardware is permitted to be used in the processing or storage of customer data. Only authorized Users may operate ISDC computer equipment.
11. **Unauthorized Access.** Unauthorized access of email, data, and the use or disclosure of another User's passwords is strictly prohibited. For example, Users are prohibited from accessing another User's files or communications without any legitimate business purpose (e.g., to satisfy idle curiosity or to "snoop"), regardless of the security designation assigned to a particular file or communication.
12. **Misrepresentation.** Technology Resources may not be used to misrepresent, obscure, suppress, or replace one's identity or the origin of data or communications. For example, "spoofing" -- constructing electronic communications to appear to be from somebody else -- is prohibited. Each User's name, email address, organizational affiliation, time and date of transmission, and related information included with electronic communications (including postings) must always reflect the true originator, time, date, and place of origination, as well as the original message's true content.
13. **Chain Letters.** Technology Resources may not be used to transmit junk mail or spam (the same or substantially similar messages sent to a large number of recipients for commercial purposes unrelated to ISDC) or pyramid schemes of any kind.
14. **Limited Liability.** ISDC will not be responsible to Users for any damages, direct or indirect, arising out of the use of its Technology Resources.
15. **Acknowledgment.** All officers, managers, supervisors and all other employees who are authorized to use Technology Resources must sign the attached Acknowledgment and Statement of Agreement. The Human Resources Department will retain the Acknowledgments in Users' personnel files.
16. **Revisions and Review.** ISDC may amend, revise or depart from this policy at any time, with or without notice. This policy does not constitute, and shall not be construed as, an express or implied contract of employment.
17. **Termination at Separation.** Before each User's last day of employment, he or she must return or otherwise surrender possession of all Technology Resources (including computers, software programs, computer peripherals, electronically stored data (including all confidential and proprietary information), data storage devices, keys, and written passwords) in his or her possession, custody or control. Upon separation of employment, ISDC will terminate User access to ISDC Technology Resources.
18. **Policy Violations.** Access to and use of ISDC Technology Resources is a privilege, not a right. Users who do not comply with this policy are subject to denial of access to ISDC Technology Resources and disciplinary action up to and including discharge.
19. **Responsibilities and Questions.** The Chief Information Security Officer is responsible to ensure the development, implementation, and maintenance of the Acceptable Use Policy for Technology Resources. If you have any questions regarding any part of this policy, please contact the Information Security Team.
20. **Review of User Access.** The Help Desk is responsible to review new user accounts to ensure they are in the appropriate groups with the correct profiles during the provisioning process. They will

also verify that terminated employees user accounts are disabled or deleted. The data owners review profiles and groups quarterly.

21. **Confidential Information.** Users may not leak, place, post, e-mail, transmit or otherwise disclose confidential, non public, sensitive and/or proprietary ISDC information to anyone outside of ISDC by any means not approved by the Information Security Officer (ISO), at any time or for any reason or otherwise use Technology Resources in violation of Customer's, Client's or User's confidentiality agreement with ISDC. Users may not discuss proprietary ISDC information in Internet chat rooms or post such information on Internet message boards. Approved e-mail containing confidential, non-public, sensitive and/or proprietary ISDC data must include an approved "Notice of Confidentiality" and other necessary disclosures as approved by ISDC.

5. Data Management and Classification Policy

Purpose

InsideSales.com (ISDC) will follow an approach to develop and implement Information security policies, standards, guidelines, and procedures based on security best practice recommendations, as stated by the FFIEC and GLBA regulations. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company information assets.

Scope

The purpose of this Data Classification Policy is to provide a procedure for protecting information that is critical to the organization. All workers who may come into contact with ISDC data are expected to be familiar with this data classification policy and to use it consistently.

All employees, contractors, part-time and temporary workers, and those employed by others to perform work for, or on behalf of, ISDC, or otherwise on company premises, or who have been granted access to ISDC information or systems for a limited purpose, are subject to this.

An information asset is defined as all data, whether in the form of electronic media, physical records, or data originated, taken or summarized from these sources, that is used by the Company or in support of Company business processes, including all data maintained or accessed through systems owned or administered by or on behalf of ISDC.

Information Asset Classification

ISDC classifies information assets based on the sensitivity, criticality, and value of the information. The ISDC Data Management Guide was designed to assist ISDC personnel in protecting and properly classifying data as either, Public, Confidential or Restricted.

Classification Definition

ISDC defines information classifications based on the sensitivity, criticality, and value of the information. Company information will be classified in one of three definitions listed in the Data Management Guide.

Data Classification Guide

Classification	Public	Non-Public	Protected	Restricted
Description	General access data from the ISDC website, press releases, and other public sources	Data for which unauthorized disclosure is expected to have limited effect on ISDC operations, assets or individuals.	Data for which unauthorized release is expected to have a serious adverse effect on ISDC operations, assets or individuals.	Data for which an unauthorized disclosure is expected to have a severe or catastrophic effect on IDSC operations, assets or individuals.
Examples		Internal ISDC data; Company Documentation	Passport Data; Human Resource Data	Customer Data (PII); Social Security Number; Credit Card Number; Driver's License Number; Protected Health Information; Bank Account Number
Risk from Disclosure	None	Low	Moderate	High

Responsibilities

The Legal Department and the Chief Information Security Officer are responsible to develop, implement, and maintain the Data Classification Policy and associated standards and guidelines.

The individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using Company information assets:

- Business units have access to system resources which are only accessible to that department. The business unit is considered the data owner of any information assets created within that department. The specifically nominated owner of the data is to be designated by the owner of that business unit and is responsible to label departmental data.
- Network administrators who manage, process, or store information assets are responsible to understand the information classifications, and apply the necessary controls to maintain and conserve the information classifications and labeling established by the business units.
- Users are the individuals, groups, or departments authorized by the Owner to access information assets. Users are responsible to understand the information classifications, abide by the controls defined by the Owner and implemented by Custodians maintain and conserve the information classification and labeling established by the Owners and to contact the Owner when information is unmarked or the classification is unknown.

Enforcement and Exception Handling

Failure to comply with the Data Classification Policy and associated standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Data Classification Policy should be submitted to the Chief Information Security Officer. Exceptions will only be permitted upon receipt of written approval from the Chief Information Security Officer. Prior to official management approval of any exception request, the individuals, groups, or organizations identified in the scope of this standard will continue to observe the Data Classification Policy.

Questions or concerns about Identification and Classification should be sent to the Chief Information Security Officer or Legal department.

6. Data Storage and Transmission Policy

In order to ensure the integrity and confidentiality of ISDC Confidential and Restricted data during storage, access, and transmission, approved network security and data encryption technologies must be utilized. It is the responsibility of every ISDC employee, contractor and vendor to ensure this policy is followed.

Definitions:

- **"Data at Rest"** is defined as any data stored on a server, desktop computer, laptop, mobile device, DVD, CD or USB drive.
- **"Accessible directly from outside the company"** is defined as data that can be accessed from a non-ISDC computer or device that is external to the ISDC network either with no password or with a combination of user credentials.
- **"Secured transport protocol"** is defined as a means of transporting data where the stream of data is encrypted. Currently, ISDC utilizes WebDAV over SSL, SFTP, and VPN as secured transport protocols. Other technologies require written authorization from the ISO.
- **"Partner IP addresses"** is defined as the Internet address of the third party who will be sending or receiving data to or from ISDC.

Secure Data Storage

Mobile Devices

All mobile devices including but not limited to, Mobile Phones, PDAs and Laptop Computers that during normal use receive or store confidential ISDC information must be encrypted using an IT approved encryption utility. In addition, the ability to remotely render data unusable must be employed where possible.

Desktop Computers

All ISDC desktop computers must be physically secured so as to not allow the removal of either the computer itself or the internal hard drive. Customer sensitive data is not to be stored on the local computer hard drive.

Network File Shares

All internal network file shares designated as *Public* are only to be used to store files containing data deemed as Public within the ISDC Data Management Guide. Any files found to be in violation of the ISDC Data Management Policy may be removed at any time without warning from these locations.

All internal network file shares designated as *Departmental* must provide limited access based on job function and the "principle of least privilege" (provide the least amount of permissions required to perform daily tasks) applied through network security permissions.

All Confidential or Restricted data placed in a file share that is accessible directly from outside the company for the purposes of transmission to a third party must be encrypted using an IT approved encryption utility.

Databases

All databases must provide limited access based on job function and the "principle of least privilege" (provide the least amount of permissions required to perform daily tasks) applied through network security permissions.

All data elements classified as highly restricted require the following additional security measures.

- Highly restricted data elements must be obfuscated in all network databases. Exceptions require business justification and approval from the department VP as well as the Chief Information Security Officer.
- Access to highly restricted data elements in a clear text format requires business justification and approval from the department VP as well as the Chief Information Security Officer.
- Export of highly restricted data elements in a clear text format requires business justification and approval from the department VP as well as the Chief Information Security Officer.

Secure Data Transmission

Protected or Restricted data as defined in the ISDC Data Management Guide must never be transmitted through public channels in non-encrypted formats.

In addition to security measures detailed below, any form of transmission that contains data elements classified as highly restricted requires business justification and approval from the department VP as well as the Chief Information Security Officer.

Email transmission of Protected or Restricted information should be limited and must utilize an IT configured secure email connection.

ISDC Web applications must be protected by 128-bit SSL encryption when vendors or customers access our site externally.

Electronic file transfers of Confidential or Restricted data transmitted into or out of the company must use a secured transport protocol. The following additional security measures will also be employed for all electronic file transfers:

- All configured secured communications will be accompanied by a list of partner IP addresses that the transmissions will be coming from/going to.
- External access to Confidential or Restricted data at rest must also be secured by two factors. For example, a customer retrieving a file from ISDC must be coming from
    - 1) an authorized IP address and
    - 2) have a valid ISDC generated username and password.
- All data placed on server(s) accessible directly from outside the company will be held no longer than five (5) calendar days. If the data is not deleted by the ISDC employee who is responsible for the data transfer, an automated script will delete all data aged beyond this point on these servers.
- All user accounts for external file transfers incoming or outgoing will auto expire every ninety (90) days. In addition, accounts will be monitored and disabled after forty five (45) days of inactivity. If an account is required for greater than ninety (90) days, the business unit requesting the account will be required to re-justify the need for the account every ninety (90) days.

- Before a business user can request a secured transport mechanism be configured between ISDC and a business partner, that business user must agree to the following conditions:
    - The business unit/user requesting the transport of data is responsible for the receiving or sending of all data between ISDC and this partner.
    - The business unit/user requesting the transport of data is responsible for verifying the successful transfer of data in a timely manner (immediately up to one (1) business day).
    - The business unit/user requesting the transport of data is responsible for deleting the data from the external facing location the data was transported to/from.

Vendor and Third Party Data Transmission

Any data transmission which occurs between ISDC and a third party is to be verified as a secure channel of communication and the area where this information resides will be verified as accessible only by authorized personnel.

Security Policy / Vendor Checklist

All vendors are required to perform a security review in regard to services conducted for ISDC. A security review should encompass all of the components of an application or service including, but not limited to, the following items supporting the application:

- Application code
- Web server(s)
- Database server(s)
- Directory and authentication device(s) (e.g., Windows domain controllers, RADIUS, etc.)
- Firewall(s)
- Configuration of network operating system platforms for any of the above

All data, which falls within Non-Public to Restricted classification, must be encrypted prior to transmission in any manner.

ISDC requires that customer information be handled as Restricted data, which includes any record containing nonpublic personal information about a customer whether in paper, electronic, or other form, which is handled or maintained by or on behalf of ISDC.

7. Document Retention Policy

Policy

The Document Retention Policy identifies the record retention responsibilities of Insidesales.com for maintaining and documenting the storage of the organization's documents and records.

Insidesales.com employees are required to honor the following rules:

- Paper or electronic documents indicated under the terms for retention in the following section will be transferred and maintained according to the schedule
- No paper or electronic documents will be destroyed or deleted if pertinent to any ongoing or anticipated government investigation or proceeding or private litigation; and
- No paper or electronic documents will be destroyed or deleted as required to comply with government auditing standards (Single Audit Act).

Record and Data Retention

Data	Minimum Requirement
Customer Data on production servers	Permanently while customer is using Insidesales.com services. Upon contract termination, Customer Data will be securely deleted within 90 days.
Customer Data on encrypted backup media	7 years
Internal Employee Data	Insidesales.com follows the published federal guidelines located here.

8. Disposal of Digital and Hard Copy Information Policy

Purpose

In response to the passing of the Data Protection Act 1998, ISDC established a policy outlining the appropriate technical and organizational measures for disposal of information that is no longer required. The policy was created to conform to any legal and statutory requirements.

Scope

ISDC sanitizes or destroys digital data before the media is disposed of or released for reuse outside the organization by using approved equipment, techniques, and procedures. ISDC tracks, documents, and verifies media sanitization and destruction actions. This policy is used to prevent unauthorized individuals from gaining access to and using the information contained on the released or reused media.

Policy

The policy is created regarding data disposal and media sanitization which resides not in the media but in the recorded data. The issue of media disposal and sanitization is driven by the data placed intentionally or unintentionally on the media. Electronic media used on a system should be assumed to contain information commensurate with the data security categorization of the system's confidentiality. If not handled properly, release of these media could lead to an occurrence of unauthorized disclosure of information. Disposal of personal and Protected information must be done in a manner that is permanent (e.g., physically cutting magnetic media, shredding hard copy documents, wiping hard drives to DOD standard).

Media Sanitization Matrix

Media Type	Sanitation Technique	Physical Destruction
Paper	Placement in secured shred bins	Destroy paper using cross cut shredders
Cell Phones	Perform a full manufacturer's reset to reset the cell phone back to its factory default settings.	Shred, Disintegrate, Pulverize, Degauss or Incinerate
Tablets	Perform a manufacturer's hard reset to reset the tablet to factory state.	Shred, Disintegrate, Pulverize, Degauss or Incinerate
Routers	Perform a full manufacturer's reset to reset the router back to its factory default settings.	Shred, Disintegrate, or Pulverize
Hard Drives	Overwrite media by using ISDC-approved technology that supplies certificate for each drive meeting DOD 5220-22.M standard	Shred, Disintegrate, Pulverize, Degauss or Incinerate
USB Removable Media and SD Cards	Overwrite media by using ISDC-approved and validated overwriting technologies/methods/tools.	Shred, Disintegrate, Pulverize, Degauss or Incinerate

CDs And DVD's	See Data Classification Policy	Shred, Disintegrate, Pulverize, or Incinerate

Roles and Responsibilities

Senior management is responsible for ensuring that the resources are allocated to correctly identify types and locations of information and to ensure that resources are allocated to properly sanitize the information. The Chief Information Security Officer is responsible for ensuring that the requirements of the information security policy with regard to information disposition and media sanitization are implemented and exercised in a timely and appropriate manner throughout the organization. The business owner should ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the impact of disclosure of such information on the organization. Users have the responsibility for knowing and understanding the confidentiality of the information they are using to accomplish their assigned work and ensure proper handling of information.

Enforcement

Failure to comply with this Policy or associated guidelines and procedures can result in disciplinary actions up to, and including, termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to this policy should be submitted to the ISO. Prior to official management approval of any exception request, the individuals, groups, or organizations identified in the scope of this policy will continue to observe this Policy.

9. Removable Media Policy

Purpose

InsideSales.com (ISDC) discourages the use of removable media devices. The ease of use and high data storage capacity of these devices could place critical information assets at risk. The purpose of this policy is to establish a standard for the base configuration necessary when there is an exception to the standard practice requiring use of these devices.

Scope

This policy applies to removable media equipment owned or operated by employees of ISDC and any person on site or under contract.

Removable media can be defined as a cartridge or as disc-based storage devices which can be used to easily move data between computers.

Examples of these devices include, but are not limited to:

- External IDE/SATA and CD/DVD disk drives
- Flash memory drives (thumb/jump drive)
- Zip Drives
- Laptop CD/DVD burners
- SD, MiniSD, MicroSD cards

Removable Media Policy

All data classified as Non-Public to Restricted, by the ISDC Data Management Guide, must be encrypted using a company approved disk encryption method.

Any data copied to a flash drive or other device must be encrypted, prior to moving any data from a secure network device.

The Vice President of a Business unit must provide authorization to use removable media devices. This use will be recognized as an exception to standard business practices.

The use of removable media devices must be managed by the corporate end point protection solution.

Related Procedures

If a business unit has a laptop or pc capable of burning CDs, the business unit is responsible to:

- Request the approved encryption software from ISDC IT
- Classify and encrypt all data before it is copied to a disk.
- Remove or destroy any duplicate copy of the data, created on the local machine, during the process of copying it to the removable media.
- Encrypt all sensitive data being provided to a vendor or between departments.
- Follow department procedure to email the key or pass-phrase to the client through an encrypted email, or to deliver the encrypted data through a separate media.
- Confirm receipt of the media. This required confirmation can be in the form of an email, phone call, mail receipt, or shipment tracking.

10. Mobile Device Security Policy

A mobile device can be defined as a web-enabled device that is normally used away from fixed locations and has been manufactured specifically to be portable and usable while being moved.

Typical mobile devices include web-enabled cell-phones (smart phones) with the ability to retrieve and store emails and attachments, laptop computers, and web-enabled tablets. These mobile devices could contain corporate data such as e-mail, files, calendar items (which often include details of meetings), and even business contacts.

Purpose

It is a standard practice of InsideSales.com (ISDC) to limit the number of mobile devices used. ISDC does not encourage the use of mobile devices because it places critical information assets at greater risk. The purpose of this policy is to establish a standard for base configuration of mobile devices. Effective implementation of this policy will mitigate the risk taken by ISDC when using these devices.

Scope

This policy applies to mobile device equipment owned or operated by ISDC, its employees, and any person on site or under contract who could use a mobile device to connect to corporate assets.

When a mobile device is connected with any work system on the corporate network, it is an extension of the corporate network and is no longer just a personal device, but is subject to the Acceptable Use Policy established by ISDC, and the Mobile Device Security policy.

Policy

This policy pertains to any mobile device defined in the scope of this policy and the data referred to is any Protected or Restricted data as defined by the Data Classification Policy.

The Data Classification Policy states that “any data classified as Protected or Restricted must be encrypted using a company approved encryption method”.

Although most mobile devices do ship with some form of user-authentication capability, these mechanisms are unacceptable to ISDC. ISDC has implemented additional measures to mitigate the risks, and will not rely on default configurations of mobile devices to provide optimal levels of security.

To properly secure a mobile device, and to reduce the vulnerabilities and risks associated with the use of any ISDC-designated mobile device, the following measures are implemented:

1. Encryption
2. Authentication
3. Remote destruction and disabling
4. Backup and restore
5. Storage Workout Quality Control encryption
6. Controlled device deployment

Mobile Phones and Tablets

The default wireless settings by the manufacturers of mobile phones do not provide adequate security and leave data vulnerable to theft if left unchanged. Additional measures must be taken to mitigate the risks if the phone is lost or stolen.

To properly secure a mobile phone, and to reduce vulnerabilities and risks associated with use, the following guidelines are recommended:

- Turn off mobile phones when not in use

- Power-on password is enabled
- Password protection enabled on screen saver
- Strong password protection scheme for device and network user login
- Encryption scheme is used for wireless transmission
- Device setup and security can be remotely administered
- Device must support Exchange ActiveSync protocol
- Device can be remotely wiped or restored to factory settings
- Device supports at least an encryption standard of AES-256
- Device deployment is conducted in a consistent manner and outlined in the IT General policy and procedures

Laptop and Tablet Computers

The default wireless settings by the manufacturers of mobile computers do not provide adequate security and are vulnerable to malicious attacks if left unchanged.

The ISDC IT department is responsible for the configuration of company laptops prior to deployment or connection to the ISDC network. The following standards to reduce the vulnerabilities and risks associated with use will be employed where possible:

- Ensure Power-on password is used
- Enable user ability to manually change passwords
- Enable password protection on screen saver
- Enable strong password protection scheme for device and network user login
- Ensure two-factor authentication is used for remote access sessions
- Ensure full disk encryption is used for all data stored on and transmitted from the device
- Verify the encryption scheme used for wireless transmission is set to an ISDC approved standard
- Allow only one active network interface on a particular device.
- Lock out network access during periods of inactivity
- Obtain patches and signature file updates from the network administrator on a regular basis
- Ensure Infrared (IR) port is disabled Infrared is used in various wireless devices for transmitting information, monitoring services, and controlling applications. Leaving these devices enabled make the device vulnerable to infiltration and information hijacking.

Antivirus Software

- Install and enable approved antivirus software
- Install and update the latest virus definitions each week, and allow Live Updates
- Enable and run virus startup scan at each boot

Operating System

- Verify the operating system is ISDC approved

- Install all the latest OS security patches and fixes required by ISDC
- Install all the latest application and software security patches and fixes
- Ensure full disk encryption is used for all classified information stored on and transmitted from the device
- Disable local file and drive sharing
- Disable Internet Connection Sharing

Remote Access

- Multi-factor or Source IP authentication is required for all remote access to ISDC Infrastructure.
- Virtual Private Network (VPN) remote access requires the approval of the Department VP or the Chief Information Security Officer in addition to the following:
    - Verify certified Virtual Private Network (VPN) client is installed
    - Verify active VPN connection icon is present for successful connection attempts
    - Verify Split Tunneling is disabled on the VPN client

Security Awareness

- Ensure network users are fully trained on the risks associated with using mobile computer technology

System Security

- Ensure mobile client is using Strong password scheme for device and network user login
- Ensure wireless NICs on mobile computers are up-to-date with the latest patches and upgrades
- Disable IR ports

Wireless Settings

- Restrict wireless settings to Read Only. All pre-configured wireless settings, from the standard build, cannot add to, change, or delete
- Ensure Broadcast SSID setting is disabled X
- Ensure only an encryption scheme used for wireless transmission
- Ensure Bluetooth is disabled
- Disable Ad Hoc operation mode on wireless NICs

Device Deployment

Device deployment must be done in a consistent manner and will be outlined in a detailed procedure document by the ISDC IT Department.

11. Wireless Access Policy

Purpose

The goal of this policy is to protect Insidesales.com technology-based resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or damage to our public image. All users employing wireless methods of accessing Insidesales.com technology resources must adhere to defined processes for doing so, using approved access points. Unauthorized access to the wireless network is not allowed.

The following policy is complementary to any previously implemented policies dealing specifically with network access and remote access to the enterprise network.

In order to provide wireless access to authorized users, Insidesales.com IT must install access points in and around the facility.

"Rogue" access points are antennas that are installed without the knowledge or permission of Insidesales.com IT and are used by individuals to gain illegal access to the corporate network.

Policy

- All wireless access points within the corporate firewall must be approved and centrally managed by Insidesales.com's IT department. The addition of new wireless access points within the facility will be managed at the sole discretion of IS. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment on premises, are strictly forbidden.
- The Information Security department will occasionally conduct sweeps of the wireless network to ensure there are no rogue access points present.
- The IS department reserves the right to turn off without notice any access point connected to the network that it feels puts the company's systems, data, and users at risk.
- 802.11 access point broadcast frequencies and channels shall be set and maintained by the IT Department. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal.
- All computer equipment and devices used to connect to the Corporate network must display reasonable physical security measures. Users are expected to secure their corporate-connected devices when they are physically at their machines as well as when they step away.
- Wireless access users agree to immediately report to the Insidesales.com Information Security department any incident or suspected incidents of unauthorized access point installation.
- Use of the wireless network is subject to the same guidelines as the Insidesales.com Technology Acceptable Use Policies
- Any questions relating to this policy should be directed to Security@Insidesales.com

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12. Anti-Virus / Anti-Malware Policy

Purpose

The purpose of this policy is to provide guidelines for the installation and maintenance of anti-virus and anti-malware software as well as the resolution procedures for viruses or malware found within the ISDC corporate network.

Scope

This policy applies to all ISDC employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties utilizing the ISDC network. This policy applies to implementation of anti-virus and anti-malware software and the necessary resolution procedures.

Policy

The following guidelines are required of all ISDC computers:

- All computers must have ISDC's standard, supported anti-virus software installed.
- Anti-virus/Anti-malware software must be scheduled to run at regular intervals.
- The software shall be operated in real time on all servers and client computers.
- The software shall be configured for real time protection.
- The software and the virus pattern or definition files shall be kept up to date.
- Users shall not be allowed to shutdown anti-virus agent.
- Virus-infected computers shall be removed from the network immediately until they are verified as virus-free.
- Any activities with the intention to create and/or distribute malicious programs into ISDC's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

Related Procedures

If deemed necessary to prevent propagation of a virus or malware to other networked devices, an infected computer device shall be disconnected from the network immediately until the virus or malware has been removed. This will be done under the direction of the Chief Information Security Officer in conjunction with the affected department SVP/VP.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

13. Access Control Policy

Purpose

The *Access Control Policy* builds on the objectives established in the *Asset Protection Policy*, and provides specific instructions and requirements for the proper identification, authentication, and authorization controls necessary to access Company resources and assets.

Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on ISDC premises or who have been granted access to Company information or systems, are covered by this policy and must comply with associated guidelines and procedures.

Policy

This policy defines the way ISDC validates users who have a business need to access network resources. The policy will outline procedures for Identification, authentication, and Authorization standards used and recognized as industry best practices.

Identification

1. Each User must have a unique account identifier or user ID.
2. Working groups (i.e. accounting, programming, etc.) must not share a single user ID for system access to ensure accurate accounting of user access and actions.
3. User IDs should not be shared or used by anyone other than the User to whom they are assigned. Users will be held accountable for all activity associated with their assigned user IDs.
4. User IDs should be added, modified, and deleted in accordance with Company-approved account management processes.
5. User IDs must be disabled within twenty-four (24) hours of notification of a status change (for example, termination or change in job).

Authentication

Under no circumstances should any user reveal passwords over the phone, fax passwords to someone, send them through email, or perform any other action that could reveal a password.

If someone claiming to represent the Company contacts you and requests information that in any manner would disclose a password, be assured that the request is invalid and do not comply.

1. Each user ID or account must be assigned a password.
2. Passwords on new accounts must expire upon first login and require an immediate password change.
3. All default system and application passwords must be changed prior to placing in the production environment or connecting to a live network.
4. Authentication credentials such as passwords and tokens should not be used by anyone other than the User to whom they are assigned.

5. Passwords should conform to the following criteria where the application allows for such criteria:
    - Password length must be a minimum of fourteen (14) characters or longer.
    - Passwords should not be equal to, or a derivative of, the user ID, user real name or Company name.
    - Password history will be enforced to maintain the last 5 passwords remembered.
    - Password cannot contain any part of your username or the company name
    - Password cannot contain 3 or more consecutive characters (e.g. ‘aaa’, ‘123abc’)
    - All systems should log the date and time for all failed and successful user attempts to access the system.
    - Passwords that have been compromised as part of a previous breach will be blacklisted.
    - All passwords must be immediately changed if known to be, or suspected of being, compromised.
    - All systems should limit the number of failed log-on attempts to a threshold of five (5) before lockout occurs to the user ID.
    - All systems must require and authenticate a valid user ID and password or token, prior to granting access to network or system resources.
    - Authentication data (e.g. password files) must be protected with encryption controls to prevent unauthorized individuals from obtaining the data.

Authorization

- User access to information will be based on the confidentiality classification of the information asset.
- Users should only be authorized the level of access to information assets that is required to meet an approved business need, or to perform a prescribed job responsibility.
- Access to Protected information must be provided on a “need-to-know” basis.
- User access rights to files, directories, and other objects should be assigned on a group basis and not assigned individually, unless doing so cannot be avoided.
- Login time restrictions, whenever practical, should be set to limit the time of day when Users can be logged into the system or network.
- The following WARNING will be displayed upon each login:

    “This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity system personnel may provide the evidence of such monitoring to law enforcement officials. ”
- Administrative access must be limited to only those users that explicitly require such privileged access.
- Users with administrative responsibilities must not use a privileged account unless specifically performing actions that require an elevated privilege level.

Definitions

- **Authentication** refers to the controls for providing Users the means to verify or validate a claimed identity through the presentation of something they know (e.g., passwords), something they own (e.g., hardware token), or something they are (e.g. fingerprint, biometrics, etc.).
- **Authorization** refers to the controls for determining the resources that Users are permitted to access, based upon the permissions and privileges for which they have been authorized.
- **Confidentiality classifications** are defined in the *Information Classification Policy*.
- **Encryption** refers to a method of scrambling information to render it unreadable to anyone except the intended recipient, who must decrypt it to read it.
- **Identification** refers to the controls for providing Users the means to convey their identities through the use of pre-determined identifiers.
- **Information assets** are defined in the *Asset Identification and Classification Policy*.
- **Integrity** refers to the protection of information and systems from malicious, unauthorized, or accidental changes.
- **Protected information** refers to information that is classified as Restricted or Protected. Refer to the *Data Classification Guide* for classification categories.

Responsibilities

The Information Security Officer (ISO) or Chief Information Security Officer approves the Access Control Policy.

The Chief Information Security Officer is responsible to ensure the development, implementation, and maintenance of the Access Control Policy.

Senior management and department managers are accountable to ensure the Access Control Policy is properly communicated and understood within their respective organizational units and to define, approve and implement procedures in their business units to ensure consistency with the Access Control Policy.

Business Owners are the managers of organizational units that have primary responsibility for information assets associated with their functional authority.

When Owners are not clearly implied by organizational design, the ISO will make the designation. Owners are responsible to:

- Define processes and procedures consistent with the Access Control Policy
- Define the access control requirements for information assets associated with their functional authority
- Process requests associated with Company-approved access request procedure
- Determine the level of access and authorizing access, based on Company-approved criteria
- Ensure the revocation of access for those who no longer have a business need to access information assets
- Ensure access controls and privileges are reviewed at least annually.

Custodians are the managers, administrators and those designated by the Owner, to manage, process, or store information assets. Custodians are responsible to:

- Provide a secure processing environment that protects the confidentiality, integrity, and availability of information;
- Administer access to information assets as authorized by the Owner
- Implement procedural safeguards and cost-effective controls that are consistent with the Access Control Policy.

Users are the individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible to:

- Understand and comply with the Access Control Policy and associated guidelines.
- Follow Company-approved processes and procedures to request and obtain access to information assets.
- Ensure authorization credentials, such as password and tokens, are not written down or stored in a place where unauthorized persons might discover them and never share a password with another employee or unauthorized person.
- Report immediately to the Help Desk or the Information Security department when authorization credentials have been, or may have been, compromised.
- Maintain the confidentiality, integrity, and availability of information accessed consistent with the Owner's approved safeguards while under the User's control.

Enforcement

Failure to comply with the *Access Control Policy* and associated guidelines and procedures can result in disciplinary actions up to, and including, termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Access Control Policy* should be submitted to the ISO. Prior to official management approval of any exception request, the individuals, groups, or organizations identified in the scope of this policy will continue to observe the *Access Control Policy.*

14. Third Party Access Policy

Purpose

This policy has been implemented to extend the current resource pool outside the fulltime employees employed by ISDC. The policy includes all contractors, part-time and temporary workers, and those employed by others to perform work on Company premises or those who can remotely access network resources with a ISDC Active directory account. This includes those accessing from outside the United States and anyone who has been granted access to Company information or systems. This policy provides specific instructions and requirements for the required authentication, and authorization controls necessary to access company information assets.

Scope

This policy applies to any third party user who must have network access created to complete a specific function or role for ISDC. When an Active Directory account is created for a third party user so that they can gain access to network resources, this policy must be adhered to. This policy will include the assignment of permissions to the users following the concept of least privilege business need, which states that the account will be given access to resources only to the level which is required to meet a specific business need.

Policy

Authorization refers to the controls for determining the resources that users are permitted to access based upon the permissions and privileges for which they have been authorized. When a third party user is hired to work with ISDC, they will be restricted to only the groups related to the data they support and should only be authorized the level of access to information assets that is required to meet an approved business need or perform prescribed job responsibilities. The business owner will be responsible for informing IT the level of permissions necessary for access of the user. Standard business practices include:

1. User IDs will be added, modified, and deleted in accordance with approved account processes.
2. User IDs must meet the requirements detailed in section 4.1 Authentication
3. User IDs must be disabled within twenty-four (24) hours of notification of a status change (for example, termination or change in job).
4. User IDs will have an account expiration date that coincides with the anticipated end of employment, testing, or contract. If this date needs to be changed then it is the responsibility of the business unit to submit a help desk ticket to make the request.
5. User access rights to files, directories, and other objects should be assigned on a group basis and not assigned individually, unless doing so cannot be avoided.
6. Access to data and resources will be re-evaluated when a user changes location or has new department needs. Changes to the groups or profile for an individual will be submitted through a help desk ticket and be approved by all data owners.

Related Procedures

Owners have primary responsibility for information assets associated with their functional authority. The Owner is responsible to:

- Define processes and procedures consistent with the Access Control Standard

- Process requests associated with Company-approved access request procedure
- Determine the level of access and authorizing access based on the least privilege access model
- Ensure revocation of access for users who no longer have a business need to access data
- Ensure the access controls and privileges are reviewed at least annually.
- Ensure that the NDA and Acceptable Use policies are signed by the contractors prior to being given access to the network.
- When submitting a request for a user account, the business unit must specify a termination date for all contractors to be added to the account. Upon termination of a temporary hire or contractor, it will be the responsibility of the business unit to submit a help desk ticket to ensure that the user account has been disabled.

Responsibilities

The Chief Information Security Officer (CISO) approves the Access Control Standard.

The Chief Information Security Officer is responsible for ensuring the development, implementation and maintenance of the Access Control Standard.

Company management, including senior management and department managers, is accountable to ensure that the Access Control Standard is properly communicated and understood within their respective organizational units. Company management also is responsible to define, approve, and implement procedures in its organizational units and ensure their consistency with the Access Control Standard.

Enforcement and Exception Handling

Failure to comply with the Access Control Standard and associated guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Access Control Standard should be submitted to the ISO. Prior to official management approval of any exception request, the individuals, groups, or organizations identified in the scope of this standard will continue to observe the Access Control Standard.

Data on the network will be secure based on the premise of a need-to-know or need-to-use basis. The data owners will determine the level of access to be provided to groups and profiles. The data owners will take into account the needs of confidentiality, integrity, and availability of the data when assigning access.

15. Remote Access Policy

Purpose

The Remote Access policy has been implemented to provide secure access to ISDC critical data for those employees who require access to the ISDC network, but are not in a secure location.

Scope

This policy applies to all forms of external access to ISDC computing systems including access via the VPN service.

Policy

To ensure the security and integrity of all ISDC resources external access to internal systems is blocked by the ISDC Firewall, except for select IP addresses which are designated by the company as an exception.

Remote access will be governed by a two factor authentication process which includes:

- Something you know (password)
- Something you have (secure token)

External access to the company email system will be limited to those users who are identified as needing access based on the business, travel requirements, or corporate responsibilities.

Remote access users are subject to the same rules and guidelines as described in the Acceptable Use Policy of Technology Resources.

16. User Access Review Policy

Purpose

This policy documents the user access review framework that identifies and encompasses access to critical business applications, databases, and network shared drives. This policy also provides specifics for the frequency of periodic reporting, auditing and remediation.

Scope

This policy establishes the frequency, scope and responsibilities associated with the user access framework.

Reviews

Each application identified will have a designated business unit owner. Each business unit owner will be responsible for reviewing and approving or restricting access to programs and applications which process confidential and/or sensitive information. To support this access audit requirement, IT will provide, whenever feasible, a mechanism for reporting user access. This report will be provided to the business unit owner for review and approval. Information Security will provide a process by which the business unit owner can review and store these reports to insure auditability.

Responsibilities

The Department of Information Security, Information Technology and the individual business units jointly identify those applications requiring access controls. These controls may include separation of duties, access controls, and auditing of systems. The Business Unit Owner is responsible for control access to the application(s), however, management and monitoring of that access may be completed by IT and Information Security. The role of the security administrator for critical business applications is to add, change, and remove user permissions.

IT – Development, implement, and deliver reports detailing user access to the business unit owner. Execute requests submitted via the approved process for access, update, and/or deletions.

Business Unit – Review and approve access. If access should be removed, then submit appropriate form.

Information Security – Provide a mechanism for the storage and maintenance of quarterly reports.

Frequency

Critical, physical, application, database, and shared drive access will be reviewed quarterly.

The Information Security team provides a report to the Business Unit Owners every quarter for verification of these users. This process should take no more than 10 business days.

- The process for performing the quarterly user access review will be as follows:
    - A User Access Report will be provided to the application owner.
    - If the report is accurate and does not require any change, the application owner will respond stating their approval.

    - If changes are required, the application owner will submit a request for change to the appropriate support group and notify Information Security when the changes are completed.
    - Information Security will generate a Help Desk ticket for each quarterly review. Changes that were requested during the review will be documented and tracked within the ticket.
- Each business owner will maintain a mechanism to restrict access to programs and applications which process confidential and/or sensitive information. This mechanism will be based on quarterly audit reports provided by the Information Security team.
- IT will maintain a mechanism that allows the owner of a program or application which processes confidential and/or sensitive information to designate the set of users who can modify the program or application. This process will also be audited by the Information Security team and then reviewed and approved by the business unit owner on a quarterly basis.
- IT and the business owners, as applicable, are responsible for ensuring that new and changed programs that process confidential and/or sensitive information move from test/development to production via an auditable change control process.
- Database Administrators who establish data security roles are responsible for ensuring that access to the data through these applications is consistent with restrictions on data access.
- IT and business unit owners, as applicable, are responsible for ensuring that appropriate information security and audit controls for confidential and/or sensitive information shall be incorporated into new systems and their applications.

Enforcement

Failure to comply with this Policy, or associated guidelines and procedures, can result in disciplinary actions up to, and including, termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

17. Virtual Private Network Policy

Purpose

The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the ISDC corporate network.

Scope

This policy applies to all ISDC employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties utilizing VPNs to access the ISDC network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Policy

Approved ISDC authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*. Any connections made through the VPN must have authorization from the Department VP or CISO of InsideSales.com.

Related Procedures

It is the responsibility of vendors with VPN privileges to ensure that unauthorized users are not allowed access to ISDC internal networks.

1. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
2. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
3. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
4. VPN gateways will be set up and managed by ISDC network operational groups.
5. All computers connected to ISDC internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard. Any internal employee who must use the VPN to access the network must use the corporate anti-virus software
6. VPN users will be automatically disconnected from ISDC's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
7. Personal computers are not allowed to be connected to the ISDC network. This includes physical connection or through VPN.
8. Only ISDC-approved VPN clients may be used.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

18. Break Glass Accounts Policy

While troubleshooting a production issue, members outside the Database or Release Management Operation Teams may need access to assist in the resolution effort. For this purpose, “Break Glass” accounts will be used.

Scope

This policy applies elevated access given to any developer or business user for the purposes of providing temporary support or temporary discovery of a problem or requirements.

Policy

Break Glass accounts for all web, application, and database platforms are to follow the established "Break Glass" standard set forth and maintained by IT.

19. Property Removal Policy

Purpose

The Property Removal Policy has been established to ensure that ISDC Hardware Assets, Confidential Information, and Intellectual Property are appropriately protected against unauthorized removal from company premises.

Policy

The removal of all packages, boxes, and hardware assets from company premises are prohibited unless approved by an ISDC Manager. Property removal may only occur between the hours of 8:00 AM and 5:00 PM local time.

The ISDC IT, Facilities and Mailroom Departments that relocate packages, boxes and hardware assets between ISDC buildings as part of their normal daily activities are exempt from this policy.

20. System Audit Log Policy

System audit logs are integral in identification of abuse and/or support issues. The integrity and retention of those log files must be actively managed at all times. Any exceptions must be noted, tracked, periodically reviewed and approved by the head of Information Security.

System Audit Log Access Restrictions

Access to the system audit logs in the production environment must be restricted to only Infrastructure and Operations personnel, Information Security personnel, and IT Management on an "as-needed" basis and isolated to only the appropriate regions of the environment relevant to the individual's role(s) within the organization.

Temporary exceptions can be granted to other parties under the direct supervision of an authorized staff member. Temporary exceptions can only be granted by a member of IT Management (i.e. VP or higher) or by the head of Information Security.

A segregated security audit log server exists that is controlled and administrated by the Information Security team and contains sensitive security logs from production servers. Access to the Security audit log server is limited to individuals within the Information Security Team.

Any modification to the source audit logs is strictly prohibited unless explicitly approved by the head of Information Security with supporting details on the scope and reason for modification. Any attempt to modify these logs without the appropriate approvals will result in disciplinary action and may include termination of employment.

System Audit Log Requirements

1) Underlying requirements

Where systematically feasible, systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including where or on what system the activity was performed from (subject)?
- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was the activity was performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

2) Activities to be logged

Where systematically feasible, logs will be created whenever one of the following activities is requested to be performed by the system:

- Create, read, update, or delete confidential information, including confidential authentication information such as passwords
- Create, update, or delete information not covered in #1
- Initiate a network connection

- Accept a network connection
- User authentication and authorization for activities covered in #1 or #2 such as user login and logout
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
- Application process startup, shutdown, or restart
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or antispyware system

3) Elements of the log

Such logs shall identify or contain at least the following elements where available, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

- Type of action – examples include authorize, create, read, update, delete, and accept network connection.
- Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
- Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation. Before and after values when action involves updating a data element, if feasible.
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
- Whether the action was allowed or denied by access-control mechanisms.
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4) Formatting and storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following:

- Microsoft Windows Event Logs collected by a centralized log management system

- Logs in a well-documented format sent via syslog, syslog-ng, or syslog reliable network protocols to a centralized log management system

5) System Audit Log Retention

System audit logs in the production environments must be configured to be retained for a minimum period of one year from the date of the event. It is imperative that the system audit logs be readily accessible for analysis during the retention period to ensure timely investigation of issues/incidents. Exceptions must be noted and approved by the head of Information Security.

21. Intrusion Detection and Prevention Policy

This policy establishes the requirements regarding intrusion detection and security monitoring to protect resources and data on the production network. It provides guidelines about intrusion detection implementation of the production networks and hosts along with associated roles and responsibilities.

Intrusion Detection System

The objectives of the IDS are:

- Increase the level of security by actively searching for signs of unauthorized intrusion.
- Prevent the loss of confidentiality of production data on the network.
- Preserve the integrity of production data on the network.
- Prevent unauthorized use of production systems.
- Keep hosts and network resources available to authorized users.

Requirements

- Host based and Network based intrusion detection systems are required within the production network. This includes host based IDS on all application, web, database, and devops servers.
- Logging from Host based IDS shall be aggregated to a SIEM solution for analysis.
- Audit logs from perimeter network security devices (load balancers, firewalls) will be aggregated to the security log server
- Intrusion Prevention systems should be enabled where available on perimeter devices

Monitoring Access to Sensitive Data

Access to critical information will be monitored by the IT security team. The IT department will assist data owners in designing controls to record, report, and follow-up on unauthorized access attempts and exception reports. Exception reports and violation logs will be monitored regularly as established by the data custodians. Whenever possible, access that occurs as a result of the use of a domain administration Account, rather than a specific account ID, will always be logged and monitored.

Internal Audits

The ISDC Information Security team will conduct routine reviews of a sample population of company computers on a quarterly basis to ensure they are in-line with company policies and procedures.

External Audits

The ISDC Information Security team will conduct regularly scheduled external network assessments using approved tools. Assessments will be conducted on a regular basis or when there is a major configuration change implemented by the IT department.

ISDC will also contract the services of a third party security team to conduct annual external security assessments.

22. Vulnerability Assessment Policy

Purpose

To mitigate the threat of security related risks, ISDC will conduct periodic assessments to discover potential vulnerabilities, determine the degree of risk associated with the possible exposure and ensure corrective actions are taken to lessen the risk.

Scope

A device is defined as any electronic system plugged into the network that either stores or routes electronic data. These devices include, but are not limited to, servers, desktop computers, routers, and switches.

Policy

A weekly scan will be performed on all external devices found in the ISDC production perimeter. Network-based Vulnerability Assessments will be conducted on ISDC trusted networks and on a weekly basis. A technical assessment of ISDC systems will be performed to identify vulnerabilities such as unused services, software vulnerabilities, access requirements, open ports, and compliance with regulated state and federal security standards.

- Vulnerability Assessments will be conducted weekly.
- Scans may also be scheduled to be run ad-hoc as warranted.
- Administrative controls such as documentation, process, procedure, and operations will be reviewed annually.
- Vulnerability risks must be ranked and addressed in order from most critical to least.
- The Information Security team is responsible to relay the results to the correct team for corrective actions to be taken based on the risks associated with the identified vulnerabilities.