WRITTEN INFORMATION SECURITY PROGRAM (WISP)

FORMS, TEMPLATES & REFERENCES

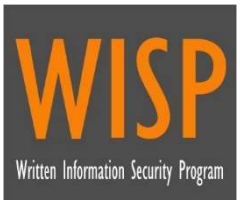

TABLE OF CONTENTS

Written Information Security Program (WISP) Implementation

ACME Business Consulting, Inc. (ACME) is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every ACME user who interacts with data and information systems. The reason for implementing ACME's Written Information Security Program (WISP) is not to impose restrictions that are contrary to ACME's established culture of openness, trust, and integrity, but to strengthen ACME's ability to guard against unauthorized access to, alteration, disclosure or destruction of data and information systems. This also includes against accidental loss or destruction.

The purpose of the Written Information Security Program is to ensure that security controls are properly implemented and that clients and business partners are confident their information is adequately protected. Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Therefore, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – This security component addresses preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – This security component addresses the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – This security component addresses ensuring timely and reliable access to and use of information.

The WISP establishes the foundation for the Information Security Program at ACME . The formation of the policies is driven by many factors, with the key factor being a risk. These policies set the ground rules under which ACME shall operate and safeguard its data and information systems to both reduce risk and minimize the effect of potential incidents.

These policies, including their related procedures, standards, and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure ACME users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help ACME comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of ACME data.

It is the responsibility of every user to know these policies and to conduct their activities accordingly. The WISP is effective as of [enter date policy is effective].

Respectfully,

[owner/manager's signature]
[insert owner/manager's printed name]
[insert owner/manager's title]

ACME Business Consulting, Inc.
(ACME)

Written Information Security Program Acknowledgement

I, _____, acknowledge I have read ACME's Written Information Security Program (WISP). I agree to abide by ACME's policies, standards, and procedures.

I acknowledge that if I do have any questions regarding any information within ACME's WISP, it is my responsibility to address those issues with my manager for further clarification. I acknowledge that ignorance on my part is not an excuse and I take full responsibility for my actions and the actions I fail to do. I acknowledge and understand that failure on my part to practice due care and due diligence may also result in the termination of my employment for cause.

I agree to indemnify, defend and hold harmless ACME , its subsidiaries and affiliated companies, and each of its respective owners, officers, directors, managers, employees, shareholders and agents (each an "indemnified party" and, collectively, "indemnified parties") from and against any and all claims, damages, losses, liabilities, suits, actions, demands, proceedings (whether legal or administrative), and expenses (including, but not limited to, reasonable attorney's fees) threatened, asserted or filed by a third-party against any of the indemnified parties arising out of or relating to any and all gross negligence and/or misconduct on my part.

The terms of this acknowledgment shall survive any termination of employment.

_____ _____

User Name / Title **Signature & Date**

_____ _____

User's Supervisor / Manager **Signature & Date**

ACME Business Consulting, Inc.
(ACME)

User Equipment Receipt of Issue

Item	Description	Qty	Make	Model	Serial #	Notes
1	Desktop					
2	Monitor					
3	Laptop w/ power cord					
4	Laptop case					
5	Docking station					
6	Cell phone w/ charger					
7	Printer					
8	Scanner					
9	Tablet					
10						
11						
12						
13						
14						
15						

Ownership:
I acknowledge that the item(s) listed in the table above, including all applicable software and licenses, remain the property of ACME . These information assets are to be used solely in the execution of my official duties with ACME . These information assets shall be accessible to ACME upon demand and that ACME may request and receive any and all of these items in my possession at any time.

Maintenance:
I acknowledge I am responsible to for the due care and due diligence in protecting these items from loss, theft, damage or compromise. I agree to keep ACME informed of any repair or upgrade requirements.

If the loss is deemed negligent on my behalf, I understand ACME may seek financial reimbursement for the equipment based on the outcome of an investigation into the loss or damage of the information asset. I acknowledge that failure on my part to practice due care and due diligence may also result in the termination of my employment for cause.

I acknowledge my responsibilities for the equipment listed above, and I verify the accuracy of the information associated with the items listed above (e.g. quantity, make, model, and serial #).

User Name / Title _____ **Signature & Date** _____

User's Supervisor / Manager _____ **Signature & Date** _____

WISP TEMPLATE 4: SERVICE PROVIDER NON-DISCLOSURE AGREEMENT FORM

This Nondisclosure Agreement (the "Agreement") is entered into by and between ACME ("Disclosing Party") and _____("Receiving Party") for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and confidential information ("Confidential Information").

1. Definition of Confidential Information. For purposes of this Agreement, "Sensitive Information" shall be defined as:

> Technical and business information relating to proprietary ideas, patentable ideas and/or trade secrets, existing and/or contemplated products and services, research and development, production, costs, profit and margin information, finances and financial projections, customers, Personally Identifiable Information (PII), clients, marketing, and current or future business plans and models, regardless of whether such information is designated as "Sensitive Information" at the time of its disclosure.

2. Exclusions from Confidential Information. Receiving Party's obligations under this Agreement do not extend to information that is: (a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party; (b) discovered or created by the Receiving Party before disclosure by Disclosing Party; (c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or (d) is disclosed by Receiving Party with Disclosing Party's prior written approval.

3. Obligations of Receiving Party. Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party. Receiving part is responsible for ensuring the confidentiality and integrity of the data. Receiving Party shall carefully restrict access to Confidential Information to employees, contractors and third parties as is reasonably required and shall require those persons to sign nondisclosure restrictions at least as protective as those in this Agreement. Receiving Party shall not, without prior written approval of Disclosing Party, use for Receiving Party's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of Disclosing Party, any Confidential Information. Receiving Party shall return to Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing.

4. Time Periods. The nondisclosure provisions of this Agreement shall survive the termination of this Agreement and Receiving Party's duty to hold Confidential Information in confidence shall remain in effect until the Confidential Information no longer qualifies as a trade secret or until Disclosing Party sends Receiving Party written notice releasing Receiving Party from this Agreement, whichever occurs first.

5. Relationships. Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venture or employee of the other party for any purpose.

6. Severability. If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as for best to effect the intent of the parties.

7. Integration. This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations and understandings. This Agreement may not be amended except in writing signed by both parties.

8. Waiver. The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

This Agreement and each party's obligations shall be binding on the representatives, assigns and successors of such party. Each party has signed this Agreement through its authorized representative.

Service Provider: _____

Name: _____ Signature: _____
(Typed or Printed Name) (Signature)

Date: _____

ACME Business Consulting, Inc.
(ACME)

Change Management Request Form

Change Request Type:
☐ Software ☐ Hardware ☐ Interface

INSTRUCTIONS
Completed forms should be submitted to your primary supervisor. Your supervisor will forward this to the IT department.

End User Information

End User Name: _____ Phone: _____

Department: _____ Email Address: _____

Machine Location

Please list the room of the machine(s) which are affected by this change requests.

Machine Location:

Software

Platform: ☐ **Windows** ☐ **Macintosh** ☐ **Linux**

Existing Software: Application Name: _____ Version: _____

Description of Issues:

New Software: Application Name: _____ Version: _____

Important Note: A copy of the license and software for each new software request must be submitted with this change request for non site-licensed software

Hardware (Additional Peripherals)

Type of Machine: ☐ PC ☐ Macintosh ☐ Linux

Type of Peripheral: ☐ Printer ☐ Scanner ☐ Other – please specify:

Description of Issues:

New Hardware: Make/Model: Serial No:

Requestor Signoff

As the end user specified on this form, I certify that the information provided in this document is both true and accurate. I also certify in the case of software changes that my department is in possession of sufficient licenses for the application.

The end user also recognizes they may be called upon to provide further information to complete this request. ACME will undertake all best efforts to ensure that changes are implemented within the appropriate timeframe. However, the end user recognizes that should the end user fail to provide assistance in a timely manner when asked there will be unavoidable delays in the deployment of the requested changes.

End User Signature **X** Date: / /

End User's Supervisor

Completed By: (print name) Signature: **X** Date Received: / /

IT Systems Administrator Use Only

Received By: (print name) Signature: **X** Date Received: / /

Change Control Board Use Only

Type of change: ☐ Minor/Pre-approved ☐ Major

CCB Outcome: ☐ Not Approved ☐ Approved

Approved By: (print name) Signature: **X** Date Approved: / /

By the very nature of every incident being somewhat different, the guidelines provided in this Incident Response Plan (IRP) do not comprise an exhaustive set of incident handling procedures. These guidelines document basic information about responding to incidents that can be used regardless of hardware platform or operating system. This plan describes the stages of incident identification and handling, with the focus on preparation and follow-up, including reporting guidelines and requirements.

PLAN OBJECTIVES

The objective of Incident Response Plan (IRP) is to:

- Limit immediate incident impact to customers and business partners;
- Recover from the incident;
- Determine how the incident occurred;
- Find out how to avoid further exploitation of the same vulnerability;
- Avoid escalation and further incidents;
- Assess the impact and damage in terms of financial impact and loss of image;
- Update company policies, procedures, standards and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

INCIDENT DISCOVERY

Malicious Actions	Possible Indications of an Incident
Denial of Service (DoS) Examples	**You might be experiencing a DoS if you see…**
Network-based DoS against a particular host	• User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	• User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	• User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses

FEDERAL RULES OF CIVIL PROCEDURE (FRCP)

Recent amendments to the United States Federal Rules of Civil Procedure (FRCP) address the discovery of Electronically Stored Information (ESI). ESI is commonly referred to as "e-discovery," which expands the use of a "legal hold" beyond the preservation of paper documents. The amendments were written in anticipation of legal arguments and tactics related to the production of ESI, such as the cost and difficulty of producing such ESI and claims that such ESI was missing, deleted, or otherwise inaccessible when it really wasn't the case. These changes took effect December 1, 2006 and require organizations to hold all electronic records until each legal matter is formally settled, even if an organization only reasonably anticipates litigation.

An organization has a duty to preserve relevant information when it learns, or reasonably should have learned of pending or threatened litigation, or of a regulatory investigation. In order to comply with its preservation obligations, the organization should inform records custodians of the respective custodian's duty to preserve relevant information. Greater leniency will be granted to those organizations who manage their information with "good faith practices." A foundation of sound, well-constructed audit trails with actionable results will go a long way in the demonstration of good faith practices.

LEGAL HOLD

A legal hold is initiated by a notice or communication from legal counsel to an organization that suspends the normal disposition or processing of records, such as backup tape recycling, archived media and other storage and management of documents and information. A legal hold will be issued a result of current or anticipated litigation, audit, government investigation or other such matter to avoid evidence spoliation. Legal holds can encompass business procedures affecting active data, including, but not limited to, backup tape recycling.

Once an organization is served with a litigation notice, all future relevant electronic communication is also subject to the legal hold.

ELECTRONIC DISCOVERY

The process of identifying and eliminating non-relevant documents while identifying and preserving the needed documents out of a set of potentially relevant documents is "culling." The relevant documents for the case are identified and preserved in a physical repository of relevant or potentially relevant documents subject to the legal hold.

The Electronic Discovery Reference Model (EDRM)[1] should be the standard used to conduct e-discovery operations. The purpose of the EDRM model is to outline guidelines for the identification of ESI in discovery. This publicly-available guide is designed to provide a baseline for e-discovery investigations. Depending on the information discovered, some areas may require a more in-depth investigation.

There are 3 key areas of focus the EDRM takes into consideration:

- Records management personnel;
- Potential custodians; and
- Information management personnel.

[1] Electronic Discovery Reference Model - http://www.edrm.net/resources/standards/identification