



Harford Technology Corporation

General Security Practices – Version 0.72

Abstract

Harford Technology Corporation as well as our clients will undoubtedly fall under a microscope of many competitors. Industrial espionage is NOT uncommon in the realm of startup or established companies. Therefore, we must protect intellectual property just as aggressively as the infrastructure and systems.

This is not meant to be a definitive set of instructions but rather a framework for the necessary awareness of non-technical threats.

As new threats and techniques evolve, this document will be updated to reflect the new information.



© 2003 Harford Technology Corporation. All right reserved.

The information contained in this document represents the current view of Harford Technology Corporation on the issues discussed as of the date of publication. Because of the dynamic nature of business computing environments, Harford Technology Corporation cannot guarantee the accuracy of any information presented after the date of publication and/or delivery.

Harford Technology Corporation makes no warranties, express or implied, in this document.

Harford Technology Corporation is a registered trademark of Harford Technology Corporation. Other product or organizational names mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract	1
Distribution	7
Document Update Process	7
Contributors	7
Documentation	8
Creation	8
Disposal	8
General	8
Physical Security	9
General	9
Conference Rooms/Offices	10
Email	11
Phones	11
Employee NDA	11
Vendor/Corporate NDA	11
Desktop Systems	12
Laptops	12
General Considerations	12



Distribution

This document will be presented to ALL Harford Technology Corporation Employees, Clients, Contractors, Consultants, and Tenants.

Document Update Process

The mechanics of an update process are TBD. However, this will require collaboration among many within Harford Technology Corporation. We will make certain that credit is given to the folks that help us keep the document up to date and aware of the latest issues

Contributors

Documentation

Creation

- A Security Classification System is under construction

Disposal

- ANYTHING that contains information relating to Harford Technology will be shredded prior to disposal. This will prevent the age-old Technique of 'dumpster diving.'
- Hand written material (ie; notes) that will be disposed of, due to its sensitive content should also contain 3-6 layers of paper below the original.
- Also, if you work at all from home, please obtain a shredder. The shredder will also be useful for maintaining personal privacy.

General

- Be aware of what is left in plain sight. Material that is considered sensitive should not be left in plain sight, on desks, copy machines, fax machines, or printers.
- Also, make an effort to keep blinds closed or at least partially closed such that we do not tempt a would-be-thief.

Physical Security

- ALL visitors must be escorted in the facility (use best judgement). Also visitors will be required to obtain and display a valid visitor's pass issued prior to entrance into the facility.
- Non-employees will NOT be granted access to the computer room at any facility
- Exceptions may be made on a case-by-case basis. The exceptions must be approved by member of Senior Management (Director Level or above). A valid example of an exception may be a Cisco Systems Engineer or a Microsoft Systems Engineer.
- There will be *NO* access to the computer room without a signed NDA
- If an exception is granted to a non-Harford Technology individual, they must be supervised at all times.

General

An ID Card system has been obtained ... ALL Harford Technology Associates, Contractors, Consultants, Vendors, Interns, and Guests will be REQUIRED to wear the Harford Technology ID 'on or above the waist' at ALL times while present at a Harford Technology facility. The information on the ID card consists of the following

- Harford Technology Logo
- Associate's Photo
- Harford Technology Classification
- Soundex representation of Associate's Name
- Return Mailing address with Guaranteed postage

The Harford Technology Classifications will be displayed as follows:

Green	- Employee
Blue	- Contractor/Consultant
Yellow	- Vendor
Red	- Guest
White	- Intern
Black	- Security

Also, feel as though it is your combined duty to challenge individuals that are not displaying a valid Harford Technology ID, and refer anyone refusing to comply to the Security Area

Entry logs have been created for both facilities to track visitors, vendors, etc. Therefore, visitors will be required to sign when entering or leaving the facility. Also, visitors will be required to display a valid visitors pass.

Conference Rooms/Offices

If sensitive material will be discussed at any meeting it is recommended that cell phones, pagers, and other types of communications equipment be deactivated and left in a controlled area outside of the meeting area

Although currently there are few areas with whiteboards visible from a window, the following are good habits to develop as we may not always meet at a Harford Technology location

- Note on the whiteboard that the material is Harford Technology Confidential
- Erase whiteboards promptly after each meeting
- Erase ALL whiteboards prior to closing the office for the evening

- Please note that ALL whiteboards will be erased and cleaned thoroughly by the janitorial staff on a daily basis

- Make certain that the room is secured. Collect all notes, handouts, etc. Also be aware of any personal items such as day-timers, PDA's etc

Also, after a meeting where confidential material is discussed (especially with a 3rd party) it may be a prudent to send an email to the attendees reminding them of their NDA and the associated commitments.

Be aware of your surroundings and what doesn't belong there. If something is out of place, take notes, such as License Number, type of car, description etc.

All offices and locations will have the expectation of a clean desk policy. This will include Securing all electronic devices (ie; Laptops, Desktops, PDA's etc). All Harford Technology proprietary documentation will be secured as well. This may be limited given the facilities, however, it is a necessary step.

Non-compliance will be reported to the appropriate supervisor.

Email

All email sent beyond the Harford Technology network will cross one or more 3rd party servers during transit. Anything deemed sensitive, such as design, financials, marketing, HR data, etc should be encrypted prior to transmission.

ALL Email -> Note at the end of the email (when appropriate) that the information is Harford Technology Corporation Confidential and Covered under the Non-Disclosure Agreement

Phones

BE CAREFUL!!! Be aware of the twists and turns of conversations. Even a seasoned individual can get 'tripped-up' talking with a professional from a Sales or Marketing organization, Trade Rag reporter, Headhunter, or someone posing as any of the previous.

- When in doubt say less!!

Telephone Security is a must! Sensitive conversations should not be conducted on a non-secure telephone. Forget the technique of trying to talk around a sensitive topic.

Employee NDA

Everyone should sign a corporate NDA. Every candidate should sign an NDA prior to any discussions beyond the job description.

Vendor/Corporate NDA

Every Vendor that will have knowledge of our strategy, or take part in strategic plans and/or product discussions should sign an NDA.

- If the vendor balks consult your Manager
- Be aware that this generally takes some amount of time.
- Also, many companies may choose not to sign or insist on revisions that make the contract useless. If this is the case, control the necessary information appropriately. (See Above)

Desktop Systems

Although the majority of today's systems are adequate, for older systems such as Windows 98 or Windows ME consider the following.

- Password protect where possible
- Use Screen Savers where possible

Laptops

Theft of laptops is rising at an alarming pace. Based on your responsibilities, select a tool such as PGP Disk to protect the Harford Technology proprietary data on your drive. If configured Properly, the would-be thief cannot gain an advantage from anything but the hardware and OS.

- A Harford Technology standard will be developed for this purpose

General Considerations

The information and policies listed above are merely a starting point. No amount of policy and/or procedures can substitute for due diligence.

THE SECURITY OF Harford Technology AND THE PRODUCTS THAT WE PRODUCE IS EVERYEMPLOYEE'S JOB!

So use your best judgment, and defer to your supervisor if necessary.

In the event that you may have any questions, please feel free to contact any member of our Security Staff. The numbers for the current staff members are listed below.

TBD
TBD
TBD