STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

Policy Title:	Confidentiality (Non-Disclosure) and Integrity of Data	
Doc Ref Number:	DTI-0065.02	
Policy Type:	Internal Only	**Page:** 1 of 8
Synopsis:	Employees and contractors working for the Delaware Department of Technology & Information (DTI) have unique access to citizen, customer and employee records, communications and data storage equipment. This policy establishes expectations and standards of behavior in safeguarding information that others entrust to us. Employees and contractors are required to take all necessary precautions not only to prevent unauthorized disclosure or modification of State computer files, but will bring to the attention of their immediate supervisor any situation which might result in, or create the appearance of, unauthorized disclosure or modification of State data.	
Authority:	Delaware Title 29, Chapter 90C, § 9002C. Establishment of the Department of Technology and Information. A Department of Technology and Information is established to replace the Office of Information Services within the Executive Department, and shall have the powers, duties and functions vested in the Department by this chapter. (73 Del. Laws, c. 86, § 1; 74 Del. Laws, c. 128, § 11.)	
Applicability:	All organizational elements of the Department of Technology and Information, including but not limited to: – DTI Employees – Any consolidated staff from other organizations – State Employees working within DTI – Contractors and private organizations providing products, services and/or support.	
Effective Date:	December 7, 2005	
POC for Change:	Chief Security Officer	

POLICY

A Message to All DTI Employees/Contractors

Our jobs at the Delaware Department of Technology & Information (DTI give us unique access to citizen, customer and employee records, communications and data storage equipment. We are trusted to use their information with care. We will carefully handle both DTI information and information that others entrust to us. Each of us is responsible for upholding the DTI's commitment to the highest standards of business conduct.

DTI employees/contractors will take all necessary precautions not only to prevent unauthorized disclosure or modification of State computer files, but will bring to the attention of their immediate supervisor any situation which might result in, or create the appearance of, unauthorized disclosure or modification of State data.

Because this agreement cannot address every situation and issues continue to evolve in our rapidly changing environment, you can seek assistance; discuss concerns or report violations through numerous channels, including your supervisor or Team Leader.
You are accountable for familiarizing yourself with this agreement:

Read: the agreement and give careful attention to those subjects that most pertain to your job duties.

Understand: the purpose of this Confidentiality and Non-disclosure Agreement and your overall responsibilities for DTI's standards of business conduct.

Consult Related Documents: employees/contractors should review and understand related DTI policies, including those governing "Acceptable Use", "FOIA", "e-Records Request", "Data & UserID Security", "Data Classification Policy" and "Disposal of Electronic Equipment/Storage Media."

Acknowledgement: employees/contractors must attest to their compliance by signing the Confidentiality and Non-disclosure acknowledgement form. See appendices 1 & 2.

Introduction

DTI employees are responsible for safeguarding the confidentiality and integrity of data in State computer files regardless of the source of those data or the medium on which they are stored; e.g., printed page, photocopies, or tape or disk. Computer programs developed to process State Agency data will not be modified without the knowledge and written authorization of that State Agency's Representative. All source data submitted by any State Agency to the Department of Technology and Information, and all data generated from the original source data, shall be the property of the State of Delaware. The control of the disclosure of those data shall be retained by the State Agency and DTI.

Note: References to "customers" in this document include the agencies/organizations we serve, citizens, and DTI employees

Applicability

DTI's expectations for responsible conduct are applicable to all parties who work on behalf of DTI, including, but not limited to, its employees, consultants, in-house contractors, and employees of vendors completing work on behalf of DTI.

Corrective Action and Discipline

Employees who violate DTI policies and standards may be disciplined up to and including dismissal, as well as be subject to civil and criminal charges. If misconduct occurs, DTI is committed to taking prompt and responsive action to correct the situation and discipline responsible individuals.

Management employees may be disciplined if they condone misconduct, do not report misconduct, do not take reasonable measures to detect misconduct, or do not demonstrate the appropriate leadership to ensure compliance.

DTI has no authority to discipline consultants, in-house contractors, and employees of vendors completing work on behalf of DTI, but expects the same level of compliance and will take the appropriate steps to ensure any misconduct is appropriately addressed.

STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

Compliance with Privacy Laws

We have a responsibility to our customers (agencies, citizens, employees) to comply with all applicable privacy laws and regulations. We should not listen -nor allow others- to customer conversations or monitor data transmissions unless it is part of our job responsibilities, and even then, only in compliance with applicable law. We should not tamper with or intrude upon conversations using wiretaps or other methods, except when authorized by law. We will neither confirm nor deny to customers or to any unauthorized person the existence of, or any information concerning, a subpoena, warrant or court order for communications, wiretaps and/or records, unless authorized by law. **During the course of employment, employees may receive a subpoena or similar inquiries from law enforcement or the government requesting or directing them to furnish records or information in the possession of DTI, including records or other customer-specific data. Employees should provide these requests immediately to their Team Leader or directly to DTI's FOIA Coordinator (Office of the CIO Executive Secretary).**

Question – A neighbor is working on a committee to help elect a new state representative. Her committee needs voter registration information for the communities in our area. She has asked me to help out by providing that information. Is it OK to try to get this information for my neighbor?

Answer - NO. You should never use your position at DTI to access information that is not available directly to the public. You should direct your neighbor to the Department of Elections who ensures all requests for voting information complies with Delaware law.

We Safeguard Customer Information

DTI possesses sensitive, detailed information about customers who trust us to safeguard that information. Any inappropriate use of confidential customer information violates that trust and weakens our relationship with our customers. For these reasons, it is a serious breach of our policies, and in some cases of the law, to use customer information for anything other than DTI business purposes. Accessing customer records, unless there is a valid business purpose, or divulging this information to any other persons, including friends, co-workers or former employees, is inappropriate. Unless we have a supervisor's express approval, we should never access our own accounts, or those of our relatives, friends, or co-workers.

Question - A friend of mine in the real estate business has asked me for some confidential information on a renter who skipped out owing three months' rent. Through my job, I have access to the information my friend needs. Can I give it to my friend?

Answer - Absolutely not. You should refuse to provide that information to your friend. Our policies prohibit using confidential information for anything other than legitimate DTI business purposes. Even requests from law enforcement or governmental agencies must always be referred to the DTI FOIA Coordinator.

U.S. Government Classified and National Security

Some of our employees have access to information covered under the U.S. Espionage Act and other regulations that govern our work with U.S. classified and national security information and impose stringent penalties for misuse of this information.

We will protect U.S. Government classified and national security information by:

- Ensuring that access to this information is restricted only to employees with proper clearance and a "need to know".
- Safeguarding this information and other assets related to national defense from others, whether such items are classified or unclassified.

- Coordinating all activities related to this information, such as proper clearance and contracts, with DTI Security.

Protecting Information

We will safeguard information in the possession of DTI by:

- Following DTI policies and procedures for identifying, using, protecting and disclosing this information.
- Properly returning, destroying or otherwise disposing of Information when it is no longer of use.
- Utilizing a "confidential" marking as appropriate for Information classified as "confidential, secret, or top secret", and ensuring that this information retains its labeling when reproducing any portion of it.
- Keeping "confidential, secret, or top secret" Information in protected places (such as secured offices, locked drawers, and password-protected computer systems).
- Taking appropriate precautions when transmitting "confidential, secret, or top secret" Information, either within or outside the DTI. In general, we should ensure that Information is not transmitted through unsecured e-mail, posted onto the Internet or sent to unattended fax machines.
- Complying with any agreements regarding the use and protection of Information.
- Protecting information owned by others. We are responsible for knowing what these agreements require of us.
- Only disclosing Information according to agreed-upon terms, generally as outlined in non-disclosure agreements between the DTI and others, or according to directives from DTI representatives authorized to permit disclosure of Information.
- Informing our Supervisor or Team Leader if we believe that any Information has been or is being used or disclosed improperly.

Question - Because I work for the State, sometimes my family or friends ask me to get information about someone's vehicle tag number. Is this appropriate?

Answer - No. You should never use your job with DTI to obtain information that isn't available to the public.

Releases of and Requests for DTI Information

We will only release DTI Information under the following conditions:

- To employees who have a legitimate, business-related need to know the DTI Information, and who have been advised of the applicable confidentiality requirements.
- To outside parties, whom we expect will treat the information appropriately,(for example, consultants, suppliers, joint venture partners) to whom disclosure has been specifically authorized and who have entered into a written agreement to receive DTI Information under terms and conditions that restrict use and disclosure of the DTI Information.
- In such a way that we are assured of the security of that disclosure. For example, we will avoid sending DTI Information to unattended fax machines or across unsecured e-mail.

We never release DTI Information or information that could be perceived as DTI Information:

- In public Internet forums, such as in chat rooms or on electronic bulletin boards;

- **When outside parties, such as the media, or outside attorneys request DTI Information, we will not respond to this request but will inform our Supervisor or Team Leader about the request and take a call back with the requesting party.**

Employee Separation

When leaving the DTI's employment, we must understand our responsibilities to:

- Return any DTI Information in our possession.
- Not take any DTI Information or copies with us.
- Continue safeguarding DTI Information and not disclose it to or use it for the benefit of other parties, including future employers, without DTI's specific prior written authorization.

Reporting Improper Disclosures and Use

We will report any improper disclosures or unauthorized use of DTI Information. Timely reporting of improper disclosures or unauthorized use can assist us in minimizing any damages; including informing certain parties of their duties to protect the DTI Information or taking other measures that protect our interests.

Privacy Principles

DTI has adopted ten "Privacy Principles" which reflect the DTI's commitment to safeguarding customer privacy in an era of rapidly changing communications technology and applications. We should be aware of these Principles and how they impact our jobs.

General Privacy Principles

1. DTI obtains and uses individual customer information for business purposes only.
2. DTI will only disclose information with the permission of the customer or as directed by a court order.
3. DTI complies with all applicable privacy laws and regulations.
4. DTI will safeguard <u>all</u> information and assets related to national defense.
5. DTI strives to ensure the integrity of all data and information entrusted to us.
6. DTI considers privacy implications as new services are planned and introduced and informs customers of the privacy implications of these services.
7. All DTI employees are responsible for safeguarding individual customer communications and information.
8. DTI participates in and supports consumer, government and industry efforts to identify and resolve privacy issues.
9. DTI will properly return, dispose of, or destroy information when it is no longer of use.

10. Each DTI employee and contractor is responsible for implementing these Principles.

DEFINITIONS

Information

For purposes of this policy, Information is:

- any and all data/information that has been entrusted to us by other agencies and organizations. Control of the disclosure of this data remains with the agency/organization.
- any and all data/information owned by DTI but not previously released to the public.

DEVELOPMENT AND REVISION HISTORY

Initial version established December 07, 2005.
Revision 1 published March 21, 2007 & July 16, 2007.
Revision 2 dated 11/1/2016 (Logo & formatting)

APPROVAL SIGNATURE BLOCK

On File James Collins	
Name & Title: Cabinet Secretary – State Chief Information Officer	**Date**: January 3, 2006

LISTING OF APPENDICES

Appendix 1 – Employee Acknowledgement Certification
Appendix 2 – Contractor Acknowledgement Certification

STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

Appendix 1 – Employee Acknowledgement Certification

State of Delaware
DEPARTMENT OF TECHNOLOGY AND INFORMATION
William Penn Building
801 Silver Lake Boulevard
Dover, Delaware 19904

DTI Employee Confidentiality (Non-Disclosure) and Integrity of Data Agreement

This is to certify that I have read and agree to abide by the guidelines set forth within the DTI Confidentiality (Non-Disclosure) and Integrity of Data Policy. As an employee of the State of Delaware, I fully intend to comply with this policy realizing that I am personally liable for safeguarding information in the possession of the State of Delaware and subject to the corrective action and/or discipline described in this agreement, up to and including dismissal for just cause. If I have any questions about this agreement, I understand that I need to ask my supervisor for clarification.

Name:_____

Signature:_____

Date:_____

STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

Appendix 2 – Contractor Acknowledgement Certification

State of Delaware
DEPARTMENT OF TECHNOLOGY AND INFORMATION
William Penn Building
801 Silver Lake Boulevard
Dover, Delaware 19904

Contractor Confidentiality (Non-Disclosure) and Integrity of Data Agreement

The Department of Technology and Information is responsible for safeguarding the confidentiality and integrity of data in State computer files regardless of the source of those data or medium on which they are stored; e.g., electronic data, computer output microfilm (COM), tape, or disk. Computer programs developed to process State Agency data will not be modified without the knowledge and written authorization of the Department of Technology and Information. All data generated from the original source data, shall be the property of the State of Delaware. The control of the disclosure of those data shall be retained by the State of Delaware and the Department of Technology and Information.

I/we, as an employee(s) of _____ or officer of my firm, when performing work for the Department of Technology and Information, understand that I/we act as an extension of DTI and therefore I/we are responsible for safeguarding the States' data and computer files as indicated above. I/we will not use, disclose, or modify State data or State computer files without the written knowledge and written authorization of DTI. Furthermore, I/we understand that I/we are to take all necessary precautions to prevent unauthorized use, disclosure, or modification of State computer files, and I/we should alert my immediate supervisor of any situation which might result in, or create the appearance of, unauthorized use, disclosure or modification of State data. Penalty for unauthorized use, unauthorized modification of data files, or disclosure of any confidential information may mean the loss of my position and benefits, and prosecution under applicable State or Federal law.

This statement applies to the undersigned Contractor and to any others working under the Contractor's direction.

I, the Undersigned, hereby affirm that I have read DTI's Policy On Confidentiality (Non-Disclosure) and Integrity of Data and understood the terms of the above Confidentiality (Non-Disclosure) and Integrity of Data Agreement, and that I/we agree to abide by the terms above.

Contractor Signature_____

Date: _____

Contractor Name: _____