

Document Code:	DPOTMH-E-52-P07	
Effective Date:	08-30-2022	
Document Type:	Policy	
Page Number:	1 of 7	
Department/Section:	Laboratory Department	
Document Title:	CONTROL OF PILFERAGE	

PURPOSE:

The purpose of this policy is to implement the control and reduce pilferage in the workplace.

LEVEL:

All Laboratory Personnel

DEFINITION OF TERMS:

Pilferage: It connotes small thefts performed repeatedly over a long period of time, such as an employee stealing small amounts of office supplies from their workplace.

Preventive Measures: Certain measures which may be adopted for the prevention of pilferage in the workplace.

POLICY:

Employee Pilferage Prevention:

- 1 **Promote a Positive Work Environment.** The easiest way to prevent employee theft is to establish a positive work environment. Employees who feel valued, heard, and appreciated may take more pride in their work and stay loyal to their employer.
 - 1.1 **Promote a workplace with a positive atmosphere.** Maintain a balance between transparency and positivity.
 - 1.2 Provide good benefits.
 - 1.3 Offer Perks. To help keep employees motivated throughout the day.
 - 1.4 **Reward employees for good work.** To boost spirits and encourage employees to stay honest and loyal to the organization.
 - 1.5 **Pay employees properly.** Offer competitive salaries and paid sick days. Ensure they are always paid on time.



Document Code:	DPOTMH-E-52-P07	
Effective Date:	08-30-2022	
Document Type:	Policy	
Page Number:	2 of 7	
Department/Section:	Laboratory Department	
Document Title:	CONTROL OF PILFERAGE	

- 2 **Take a preventive approach.** An employee-assistance program can help prevent workplace theft and pilferage. Provide a problem-solving forum for company employees, you may be helping to defuse their impulse to steal.
 - 2.1 Know the reason for Pilferage. Knowing the reason why employees commit pilferage. After figuring out the reason for the motive, address the root cause wherever possible.
 - 2.2 **Seminars & lectures to employees** as per designation, appointment & job description properly planned could also prove to be an effective tool. Exposing & targeting employees through such activity besides creating awareness also makes them understand the religious, moral & social responsibilities.
- 3 **Implement Checks and balances**. A simple system of checks and balances helps detect pilferage faster and prevent it from happening in the first place.
 - 3.1 Require managers to review their employees' work before a financial task is considered complete.

4 Security Protocols and Procedures

- 4.1 **Implement Security Measures.** Use security measures to make stealing more difficult. These tools not only physically restrict potential thieves, but may also deter them from even attempting to steal.
- 4.2 **Lock up high-value** inventory items, tools, cash, and medicines. Medical facilities should take extra precautions, such as two-step access (i.e. a passcode on an exterior door, then a physical lock on a safe inside).
- 4.3 **Restrict access** to financial and personal data. The fewer people who can access sensitive information, the lower your risk of theft.
- 4.4 **Install security cameras.** Position them to monitor break rooms, warehouses, stock rooms, cash registers, and isolated areas of the workplace.
- 4.5 Order a security audit of your operations. Use the results to address your organization's weak points. For example, if employees share access cards,



Document Code:	DPOTMH-E-52-P07
Effective Date:	08-30-2022
Document Type:	Policy
Page Number:	3 of 7
Department/Section:	Laboratory Department
Document Title:	CONTROL OF PILFERAGE

- switch to a passcode lock system instead. Or, if there's a blind spot in your camera coverage, reposition them or install another.
- 4.6 Install keypad or swipe card entry door. Securing offices reduces the risk that an employee's external fraud partner or a former employee can gain access to the office.
- 5 **Follow good disposal practices**. Shred sensitive documents, delete computer files, and wipe devices before passing them onto another employee.
- 6 **Restrict access to data**. Reduce the number of employees who handle or work with sensitive information, both from your company and customers. Require passwords to access financial files or programs.
- 7 **Protect devices with strong passwords**. Require employees to set passwords with at least one capital letter, one lowercase letter, one number, one special character, and eight characters in length. Remind them to change these passwords frequently (around every three months).
- 8 Remove access for terminated employees. Immediately restrict access to networks and computers.
- 9 Write Strong Policies. Clear, well-written, and comprehensive policies go far towards anti-theft efforts. Make sure your workplace policies on theft (and data theft) are strong and that you communicate them widely.
 - 9.1 **Include specific examples** of behaviors that won't be tolerated. Outline scenarios from taking home office supplies to leading a group fraud scheme.
 - 9.2 Explain why even the smallest theft incident can harm both the organization and the employee. Note the ways that the employer will suffer (reputation damage, financial harm), as well as the individual (discipline, trouble finding another job after getting caught, loss of coworkers' trust).
 - 9.3 **Outline the consequences** for violating the policies. Explain the levels of problematic behavior and the potential disciplinary actions for each.
 - 9.4 Emphasize consistency. Explain that regardless of an employee's position or length of service, they'll face the same consequences if they commit theft.



Document Code:	DPOTMH-E-52-P07	
Effective Date:	08-30-2022	
Document Type:	Policy	
Page Number:	4 of 7	
Department/Section:	Laboratory Department	
Document Title:	CONTROL OF PILFERAGE	

- 9.5 Communicate your policies well. Provide annual anti-theft training to review them and send out company-wide emails or through the communicator of the company with the policies attached whenever you update them.
- Screen Out Applicants for Hiring. Background screening of all applicants for employment.
 - 10.1 **Perform background checks and criminal record checks**. These will help you rule out applicants with a history of fraudulent or otherwise criminal behavior.
 - 10.2 **Call the applicant's references**. Ask about their behavior and reputation at their previous workplaces.
- 11 **Educate employees.** Show them how the bottom-line repercussions of theft affect the company, and encourage their help. Outline procedures for reporting theft, ensure confidentiality, and lay out the consequences of dishonesty.
 - 11.1 **Policy of conflict of interest** with an awareness program on corruption and corrupt practices could go a long way in creating the desired effects.



Document Code:	DPOTMH-E-52-P07	
Effective Date:	08-30-2022	
Document Type:	Policy	
Page Number:	5 of 7	
Department/Section:	Laboratory Department	
Document Title:	CONTROL OF PILFERAGE	

DOCUMENTATION:

New Policy

DISSEMINATION:

- 1. Unit Meeting
- 2. Weekly Middle Manager's Meeting
- 3. Policy Log Book

REFERENCES:

- HSD / DIESEL: Proper syndicates are established involving Motor Man, Drivers, Services Companies & HSD carriage contractors, following factors contribute:

 Non availability, conformance & awareness of S.O.P's on purchase, issue & consumption of HSD
- 2. Non availability of properly calibrated gauges & flow meters at Storage Tanks.
- Consumption of generators, contractor vehicles, fire pumps, contractor cranes & machinery.
- 4. Non initiation of company action upon culprits apprehended including black listing of carriage contractors.
- 5. CALPIRG (2000). Nowhere to Turn: Victims Speak out on Identity Theft. A CALPIRG/PRC Report—May. Sacramento, California: Privacy Rights Clearinghouse.
- 6. Cullier, D. (2003). "SU Study Shows Washingtonians Fear Identity Theft But Want Government to Operate in the Open." Washington State University News Service. Feb. 26.
- 7. Davis, K. (2002). "Clean up Your Trash: A Home Shredder Is Insurance Against Identity Theft." *Kiplinger Personal Finance* 56(6):102.
- 8. Economic Crime Institute (2003). "Identity Fraud: A Critical National and Global Threat." White Paper. A Joint Project of the Economic Crime Institute of Utica College and LexisNexis. Oct. 28.



Document Code:	DPOTMH-E-52-P07	
Effective Date:	08-30-2022	
Document Type:	Policy	
Page Number:	6 of 7	
Department/Section:	ection: Laboratory Department	
Document Title:	CONTROL OF PILFERAGE	

- 9. Finch, E. (2003). "What a Tangled Web We Weave: Identity Theft and the Internet." In Y. Jewkes (ed.), *Dot.cons: Crime, Deviance, and Identity on the Internet*. Cullompton, England: Willan. [Full Text]
- 10. Federal Trade Commission (2003a). Identity Theft Report. [Full Text]
- 11. Foley, L. (2003). "Enhancing Law Enforcement—Identity Theft Communication." Identity Theft Resource Center. [Full Text
- 12. Goodwin, B. (2003). "Identity Theft Is Key Cybersecurity Fear." Computerweekly.-com. April 17
- 13. Identity Theft Resource Center with Dale Pletcher (2003). Identity Theft–The Aftermath.http://www.idtheftcenter.org/library.shtml



Document Code:	DPOTMH-E-52-P07
Effective Date:	08-30-2022
Document Type:	Policy
Page Number: 7 of 7	
Department/Section:	Laboratory Department
Document Title:	CONTROL OF PILFERAGE

APPROVAL:

	Name/Title	Signature	Date
Prepared by:	MONICA B. VILLANUEVA, RN, RMT, PhD Laboratory Manager	Str. Vanue v.	9-7-22
Verified:	MELANIE ROSE B. ZERRUDO, MD, FPSP Chairman, Department of Pathology	bauge fens	4-7-20
Reviewed:	DENNIS C. ESCALONA, MN, FPCHA, FPSQua Quality Assurance Supervisor	2	09-07-2012
Recommending	ROSARIO D. ABARING, RN, MN, PhD, FPCHA Ancillary Division Officer MA. ANTONIA S. GENSOLI, MD, FPPS, FPCHA	R bung &	. 09.07.20
Approval: Vice Preside SOCORRO V	Vice President – Chief Medical Officer SOCORRO VICTORIA L. DE LEON, CPA, MBA, PhD, FPCHA Vice President- Chief Operating Officer	O MALAPITAN, MD	
Approved:	GENESIS GOLDI D. GOLINGAN President and CEO		9/0/22