

JANITORIAL EMPLOYEE THEFT & CLIENT PROPERTY RISK GUIDE

Crime Insurance • Janitorial Bonds • Employee Dishonesty • Keys • Access • Incident Response

THE QUESTION THIS GUIDE HELPS YOU ANSWER

If a customer accuses one of your employees of stealing something, what actually protects your janitorial company and your customer? Use this guide to review insurance, bonding, employee controls, customer access, and your response process.

1. Coverage Comparison: Know What You Bought

Risk / Tool	What to Review	Key Question
General Liability	Accidental property damage and applicable exclusions	Is this accidental damage or intentional theft?
Commercial Crime / Employee Dishonesty	Covered dishonest acts, covered property, who qualifies as an employee	Whose property is protected and under what conditions?
Janitorial / Service Bond	Bond terms, obligee/customer protection, covered dishonest acts	Who can recover under the bond and what proof is required?
Third-Party Crime Coverage	Coverage for customer property, definitions, limits and conditions	Does the policy address property belonging to customers?
Property Coverage	Company-owned property and applicable theft provisions	Is the stolen property ours or the customer's?

Remember: "Bonded and insured" is marketing language, not a coverage analysis. The real question is whose property the policy or bond protects, under what circumstances, and subject to what terms.

2. Employee Security & Hiring Controls

- Written hiring and screening procedures are consistently followed.
- Identity and employment information are verified according to company procedures and applicable law.
- Background-screening practices are reviewed with qualified counsel for legal compliance.
- Employees receive written rules regarding theft, customer property, keys, passwords, and unauthorized access.
- Supervisors understand how to report suspicious behavior without conducting their own unsupported investigation.
- Employees are trained not to borrow, use, remove, or relocate customer property without authorization.
- Disciplinary and termination procedures include immediate access review.

3. Key, Badge & Building Access Audit

- Maintain a current inventory of every customer key, badge, fob, alarm code, and electronic credential.
- Record who received each access device or credential.
- Limit access to only the locations and times required for the employee's work.
- Do not use shared access codes when individual credentials are reasonably available.
- Lost keys, badges, or compromised codes are reported immediately.
- Customer access instructions are stored securely.
- Physical keys are returned when an employee changes assignments or leaves the company.
- Digital access is disabled promptly when employment or a customer assignment ends.
- Periodically reconcile the access log with active employees and active customer assignments.

4. Customer Property Risk Review

- Identify accounts where employees work around high-value inventory, electronics, cash, pharmaceuticals, tools, or sensitive property.
- Identify accounts where crews work alone or after hours.
- Document customer restrictions on rooms, cabinets, desks, inventory, or equipment.

- Use supervisor walkthroughs or quality-control visits where appropriate.
- Maintain records showing which employees were assigned to each customer location.
- Review customer contracts for theft, bonding, crime, and access-control requirements.
- Discuss unusually high-value customer property exposures with the insurance professional.

5. Workforce Model & Insurance Definitions

- Review whether the crime policy's definition of employee matches the people performing work.
- Identify temporary workers, leased workers, independent contractors, and subcontractors.
- Do not assume a subcontractor is treated as an employee under a crime policy.
- Review whether dishonest acts by subcontractors require separate coverage or contractual controls.
- Require subcontractors to meet applicable crime/bonding requirements when customer contracts demand them.
- Confirm your workforce model and your insurance definitions match.

6. Theft Allegation Response

- Take every allegation seriously without treating every allegation as proven.
- Record the date, time, customer, location, property allegedly missing, and person reporting the allegation.
- Preserve schedules, access logs, time records, video, messages, and other potentially relevant information.
- Notify management immediately.
- Follow applicable policy and carrier/agency claim-reporting procedures.
- Do not promise that insurance or a bond will pay before coverage is evaluated.
- Do not accuse an employee without an appropriate factual investigation.
- Coordinate with qualified legal counsel, law enforcement, the customer, insurer, or bond provider when appropriate.
- Document corrective action and any access changes after the incident.

7. Lost Key / Compromised Access Response

- Notify the customer promptly according to the contract and incident procedure.
- Identify exactly what key, badge, fob, code, or credential was compromised.
- Determine which areas the credential can access.
- Disable electronic credentials when possible.
- Document replacement, rekeying, or access-control costs.
- Preserve records showing who had possession of the credential.
- Review whether the event may trigger insurance, crime, bond, cyber, or contractual obligations.

8. Client Access Register

Customer / Location	Key / Badge / Code	Assigned To	Issued	Returned / Disabled

9. Crime / Bond Coverage Review

Coverage / Bond	Limit	Who Is Covered?	Whose Property?	Action Needed

10. Corrective Action Plan

Exposure / Issue	Current Control	Action Required	Owner	Due Date

Your customer gave you the keys to their building. Your risk-management program should demonstrate that you understand what that trust is worth.

Important: This guide is for educational and risk-management purposes only. Crime policies, fidelity coverage, janitorial/service bonds, general liability policies, and other forms vary materially. Coverage depends on actual policy or bond terms, definitions, conditions, exclusions, endorsements, limits, and the facts of a loss. Employment, privacy, investigation, and contract issues should be reviewed with qualified counsel when appropriate.