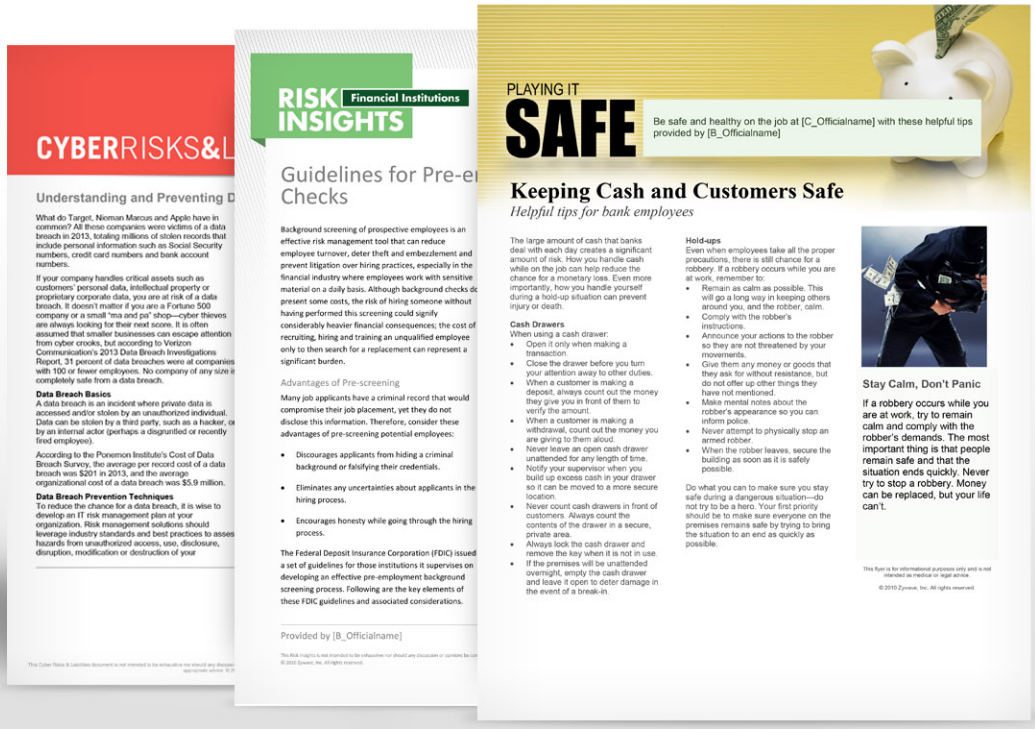
Bankers Insurance, LLC

Financial Industry Services Portfolio



Are your employees trained to identify and prevent identity theft?

Our FTC resources will help keep your team informed and compliant, and your customers safe.

Do you have the policies in place to respond to a data breach?

Financial institutions are common targets for hackers and thieves. Learn how to identify, respond to and prevent a data breach with our suite of cyber liability documents.

Are you prepared to handle a business interruption?

Theft, acts of violence and natural disasters are real-life threats to your organization. Protect your institution by creating a business continuity plan. We can help.

BANKERS INSURANCE LLC
Insuring today to ensure tomorrow.

(800) 541-1419

http://www.bankersinsurance.net/banks

4490 Cox Road, Glen Allen, VA 23233

Sample Documents

Table of Contents

Policies, Programs and Manuals

Employer Resources

Employee Safety Resources

POLICY

General Email/Internet Security and Use

Location:

Effective Date:

Revision Number:1

Purpose

The General Email/Internet Security and Use Policy forms the foundation of the corporate Information Security Program. Information security policies are the principles that direct managerial decision making and facilitate secure business operations. A concise set of security policies enables the IT team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorized behavior for personnel approved to use information assets.

Applicability

The General Email/Internet Security and Use Policy applies to all employees, interns, contractors, vendors and anyone using assets. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks and components owned or leased by or its designated representatives.

General Policies

All employees, contractors, vendors and any other person using or accessing information or information systems must adhere to the following policies.

- All information systems within are the property of and will be used in compliance with policy statements.
- Any personal information placed on information system resources becomes the property of .
- Any attempt to circumvent security policy statements and procedures (i.e., disconnecting or tunneling a protocol through a firewall) is strictly prohibited.
- Unauthorized use, destruction, modification and/or distribution of information or information systems is prohibited.
- All users will acknowledge understanding and acceptance by signing the appropriate policy statements prior to use of information assets and information systems.
- At a minimum, all users will be responsible for understanding and complying with the following policy statements:
    - General Security Policy
    - System Security Policy
    - Desktop Service Security Policy
    - Internet Acceptable Use Policy
    - Personal Equipment Policy
    - Virus, Hostile and Malicious Code Policy
- All users will report any irregularities found in information or information systems to the IT team immediately upon detection.
- information systems and information will be subject to monitoring at all times. Use of information systems constitutes acceptance of this monitoring policy.

- Use of any information system or dissemination of information in a manner bringing disrepute, damage or ill will against is not authorized.

- Release of information will be in accordance with Policy Statements
- Users will not attach their own computer or test equipment to computers or networks without prior approval of the IT team or its designated representative.

System Security Policy

's System Security Policy addresses access control, use of hardware, operating systems, software, servers and backup requirements for all systems maintained and operated by .

Applicability

The System Security Policy applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or his/her designated representative.

Password System Security

In today's information age, poorly selected, reusable passwords represent the most vulnerable aspects of information security. In fact, computer security experts estimate that 96 percent of all security breaches occur because of inadequate safeguards of network usernames and passwords. has adopted this policy to ensure that the private information of our clients and our proprietary corporate data are kept secure at all times. -authorized users must comply with creation, usage and storage policies to minimize risk to corporate information assets.

- Passwords will conform to the following criteria:
    - Passwords will be a minimum of seven characters
    - Passwords must consist of at least one uppercase letter, one lowercase letter and one number.
- The sharing of passwords is prohibited.
- Any suspicious queries regarding passwords will be reported to the IT team.
- Passwords will be protected as proprietary information. Writing them down or storing them unencrypted on the information system is prohibited.
- Users will be forced to change passwords every 90 days and may reuse passwords only after 10 different passwords have been used.
- Accounts will be locked out after five failed password attempts in a 30-minute time period. Accounts can be reset by contacting the IT team or by waiting 30 minutes for the account to reset automatically.
- Users will be forced to unlock their computers using their network password after 60 minutes of inactivity on their desktops.
- All system passwords will be changed within 24 hours after a possible compromise.
- When users leave the organization, their accounts will be immediately disabled or deleted.
- If the user leaving the organization was a privileged user or a network administrator, all system passwords will be changed immediately.

Desktop Services Security Policy

The Desktop Services Security Policy addresses the authorized and legitimate use of hardware, operating systems, software, LAN, file servers and all other peripherals used to access any information system.

- No software of any kind will be installed onto a laptop or desktop computer without the approval of the IT team.
- Only system administrators will have the ability to install software.
- Unauthorized copying or distributing of copyrighted software is a violation of Federal Copyright Law and will not be permitted.
- Personal software will not be installed on any machine.

- Users will not allow non-employees to use any machine or device without authorization of the IT team.
- The following items are corporate policy for security monitoring:
    - All systems and network activities will be subject to monitoring. Use of systems and networks constitutes consent to this monitoring.
    - Disabling or interfering with virus protection software is prohibited.
    - Disabling or interfering with logging, auditing or monitoring software is prohibited.
    - All desktop services will be subject to inventory and inspection.
    - Security irregularities, incidents, emergencies and disasters related to information or system will be reported to the IT team immediately.
- The following items are corporate policy for system usage:
    - Sabotage, destruction, misuse or unauthorized repairs are prohibited on information systems.
- All repairs will be authorized and performed by the IT team.
    - Desktop resources will not be used to compromise, harm, destroy or modify any other service or resource on the information system.
    - All data on information systems at is classified as company proprietary information.
    - Users will secure all printed material and other electronic media associated with their use of information and information systems.
    - Storage, development or the unauthorized use of tools that compromise security (such as password crackers or network sniffers) are prohibited.

Internet Acceptable Use Policy

Internet access is provided to employees to conduct business. While these resources are to be used primarily for business, the company realizes that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites during non-business hours.

- Non-business Internet activity will be restricted to non-business hours. actively blocks non-business sites during working hours. Working hours are defined as Monday – Friday from 7 a.m. – noon and from 12:45 p.m. – 5 p.m.
- The definition of non-business sites is the sole discretion of the IT team. This definition can, and will, change without notice as the Internet continues to evolve.
- Internet activity will be monitored for misuse.
- Internet activities that can be attributed to a domain address (such as posting to newsgroups, use of chat facilities and participation in mail lists) must not bring disrepute to or associate with controversial issues (i.e., sexually explicit materials).
- Internet use must not have a negative effect on operations.
- Users will not make unauthorized purchases or business commitments through the Internet.
- Internet services will not be used for personal gain.
- Internet users will make full attribution of sources for materials collected from the Internet. Plagiarism or violation of copyright is prohibited.
- Release of proprietary information to the Internet (i.e., posting information to a newsgroup) is prohibited

POLICY

Return to Work

Location:

Effective Date:

Revision Number:1

PURPOSE

This policy is in place to ensure provides meaningful work activity for employees who are temporarily unable to perform all, or portions, of their regular work assignments or duties. This policy applies to employees suffering from either work or non-work related injury or illness. The goal is to allow valued company employees to return to productive, regular work as quickly as possible. By providing temporary transitional or modified work activity, injured employees remain an active and vital part of the company. Studies show that a well-constructed Return to Work Policy reduces lost time days, allows workers to recover more quickly and makes for a more positive work environment.

SCOPE

All active employees who become temporarily unable to perform their regular job due to a compensable work related or non-work related injury or illness may be eligible for transitory work duties within the provisions of this program. Return to work tasks may be in the form of:

- Changed duties within the scope of the employee's current position
- Other available jobs for which the employee qualifies outside the scope of his or her current position
- An altered schedule of work hours

DEFINITIONS

- **Transitional duty** is a therapeutic tool used to accelerate injured employees' return to work by addressing the physical, emotional, attitudinal and environmental factors that otherwise inhibit a prompt return to work. These assignments are meant to be temporary and may not last longer than 90 days, though permits multiple 90-day assignments back-to-back if it is medically warranted.
- **Alternate duty** is a part of 's Return to Work Policy that is designed as a placement service for individuals who have reached maximum medical improvement and are still unable to perform the essential functions of their pre-injury job.

APPLICABILITY

Length of Duty

- If work is available that meets the limitations or restrictions set forth by the employee's attending practitioner, that employee may be assigned transitional or modified work for a period not to exceed 90 days. Transitional or light duty is a temporary program, and an employee's eligibility in these reduced assignments will be based strictly on medical documentation and recovery progress.

Daily Application

- An employee's limitations and restrictions are effective 24 hours a day. Any employee who fails to follow his or her restrictions may cause a delay in healing or may further aggravate the condition. Employees who disregard their established restrictions, whether they are at work or not, may be subject to disciplinary action up to and including termination.

Qualification

- Transitional or modified duty will be available to all employees on a fair and equitable basis with temporary assignments based on skill and abilities. Eligibility will be based upon completion of the Return to Work Evaluation Form by the

POLICY

Identity Theft Prevention Policy

Location:

Effective Date:

Revision Number: 1

Purpose

This policy establishes how will protect its employees, contractors, customers and the organization from damages related to the loss or misuse of sensitive information. This policy will define sensitive information, describe the physical security of data when it is printed on paper and describe the electronic security of data when it is stored and distributed.

This policy enables to protect existing customers, reduce the risk from identity theft and minimize potential damage to the company from fraudulent new accounts. The program will assist in the following:

- Identifying risks that are potentially fraudulent within new or existing covered accounts.
- Detect risks when they occur in covered accounts.
- Respond to risks to determine if fraudulent activity has occurred, and then act accordingly if fraud has been attempted and committed.

Scope

This policy applies to all employees who are exposed to identity theft risks.

POLICY GUIDELINES

Sensitive Information Policy

Sensitive information includes the following items, whether stored in electronic or printed format:

- Credit card information (credit card numbers—whole or part; credit card expiration dates; cardholder names; cardholder addresses).
- Tax identification information numbers (Social Security numbers; business identification numbers; employer identification numbers).
- Payroll information (paychecks; paystubs).
- Cafeteria plan check requests and associated paperwork.
- Medical information for any employee or customer (doctor names and claims; insurance claims; prescriptions; any related personal medical information).
- Other personal information of a customer, employee or contractor (dates of birth; addresses; phone numbers; maiden names; names; customer numbers).

Hard Copy Distribution

Each employee and contractor performing work for will comply with the following storage rules:

- File cabinets, desk drawers, overhead cabinets and other storage areas containing sensitive information will be locked when they are not in use.
- Storage rooms containing sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.

POLICY

Location:

Effective Date:

Drug-free Workplace

Revision Number:1

Purpose

recognizes that employees are our most valuable asset, and the most important contributors to our continued growth and success. We are firmly committed to the safety of our employees. will do everything possible to prevent workplace accidents and is committed to providing a safe working environment for all employees.

To further this goal, has developed a Drug-free Workplace Policy effective . The program will consist of three components: Post-Offer Drug/Alcohol Screen, Reasonable Cause Drug/Alcohol Screen and Post-Incident Drug/Alcohol Screen. This policy applies to all candidates for employment as well as all current employees. This policy also serves to reinforce the 's intolerance for illegal drug use and working under the influence of alcohol.

Post-Offer Testing

believes accident prevention and a safe work environment begin with hiring. As such, all applicants offered employment will be required to undergo a Drug/Alcohol Screening. Employment is conditional on the results of the Drug/Alcohol Screen.

Procedure

Any applicant the Company hires will be directed to the proper clinic, at Company expense, to undergo a Post-Offer Drug/Alcohol Screen. The clinic will release the results to the Human Resources Manager, who in turn will notify the candidate of the results.

The test will consist of a breath alcohol test along with a urine analysis test for any non-prescribed illegal substances listed in Exhibit 'A' below.

Consequence

In the event the drug test comes back positive, the Medical Review Officer (MRO) will review the report and contact the applicant to determine if any extenuating circumstances, relevant at the time of the test, could have resulted in a false positive. The MRO will determine if the applicant will be re-tested. If any applicant tests positive with a blood alcohol level exceeding .02 or any non-prescribed illegal substance listed in Exhibit 'A', will withdraw their offer of employment. If any applicant refuses to submit to the tests, the offer will be withdrawn.

Reasonable Cause

reserves the right under all applicable laws to test any employee for alcohol and illegal drugs if the employee shows cause. Management, supervisors and lead personnel have been trained to identify symptoms of being under the influence of illegal drugs or alcohol.

Procedure

If a supervisor, manager or lead person identifies a problem, they will ask another supervisor/manager/lead person to confirm the reasonable cause. Both persons will then individually fill out a Reasonable Suspicion Report. After filling out the report and it is decided jointly that reasonable suspicion still exists, the employee will be escorted to a private area where the supervisor/manager/lead person will speak to the person confidentially. The employee will be given a chance to explain. If, after the explanation the supervisor/manager/lead person believes the employee is unfit to perform his or her duties and reasonable suspicion for use of illegal drugs or alcohol still exists, the employee will be asked to go for a test. They will then be transported by to our designated testing facility.

RISK INSIGHTS Financial Institutions

Guidelines for Pre-employment Background Checks

Background screening of prospective employees is an effective risk management tool that can reduce employee turnover, deter theft and embezzlement and prevent litigation over hiring practices, especially in the financial industry where employees work with sensitive material on a daily basis. Although background checks do present some costs, the risk of hiring someone without having performed this screening could signify considerably heavier financial consequences; the cost of recruiting, hiring and training an unqualified employee only to then search for a replacement can represent a significant burden.

Advantages of Pre-screening

Many job applicants have a criminal record that would compromise their job placement, yet they do not disclose this information. Therefore, consider these advantages of pre-screening potential employees:

- Discourages applicants from hiding a criminal background or falsifying their credentials.
- Eliminates any uncertainties about applicants in the hiring process.
- Encourages honesty while going through the hiring process.

The Federal Deposit Insurance Corporation (FDIC) issued a set of guidelines for those institutions it supervises on developing an effective pre-employment background screening process. Following are the key elements of these FDIC guidelines and associated considerations.

Extent of Background Checks

At a minimum, it is advisable to ensure that an applicant's history does not include a criminal conviction or deferred prosecution for a specific crime, such as dishonesty, breach of trust or money laundering that would bar him or her from working in the industry in accordance with Section 19 of the Federal Deposit Insurance Act. Searches might include federal, state and county records.

> Hiring someone without having performed a background check could lead to considerable financial consequences.

Beyond the basic criminal background check, the FDIC suggests taking a risk-focused approach to determining additional levels of screening, which might include identity verification, education verification and professional license verification. The access level and sensitivity of the position will be key factors in determining whether or not additional screening is appropriate. It is advisable to maintain background checks on existing employees by continuing to perform them on a regular basis.

Sanctions Checks

The FDIC also recommends you check each federal banking agency's listing of individuals who have been

assessed civil money penalties or that have been banned from banking. Regulatory sources might include the New York Stock Exchange (NYSE), the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Asset Control (OFAC), the FBI Most Wanted Terrorist List. This initial screening stops the process if certain criteria are not met during the searches.

Employment Applications

The background check will be more efficient, more valuable and less costly if the employment application contains certain elements, such as a statement that all information is accurate and that any untruthfulness or omissions are legal grounds for termination. A standardized format that consistently collects all necessary information will also speed the background screening process. Some other helpful elements include:

- Any other names used
- Reason for leaving past positions ("disagreement" or "mutual agreement" are red flags)
- Specification that names of actual employers must be listed (staffing firms should be listed, not the firm hosting temporary workers)
- Detailed contact information for references listed

A simple way to streamline the process is to implement an online application process that requires certain fields necessary for the screening to be completed. When a need for revision arises, the form can be easily modified across the entire organization. The application can be linked directly to provider's systems that will extract all necessary information for the background screen.

Verify that all information on the application is accurate, and check credit reporting agencies for any anomalies.

Legal Duties

To simplify the task, you may find it helpful to outsource the process to a background screening service provider.

For many screening tasks, such as criminal background checks, outside providers can be faster and more thorough. It is important that when selecting such a provider, you consider financial statements and health, the provider's hiring and employment processes, identity theft safeguards and, of course, service offerings.

You have several obligations to the applicant under the Fair Credit Reporting Act (FCRA).

- Any applicant on whom an institution performs a background screen must give his or her written authorization to conduct the report.
- If you ultimately deny employment, you must provide notification through pre-adverse action and final adverse action notification letters.

For More Help

If you need more information about protecting yourself from liabilities associated with hiring and termination, contact Bankers Insurance, LLC. Our insurance experts can keep you covered and give you peace of mind.

Step-by-Step Guide to Creating an FTC-Approved Red Flag Rule Program

Step One: Identify Relevant Red Flags

When designing your Red Flag Rule Program as mandated by the Federal Trade Commission (FTC), the first step is determining the types of red flags your business faces day-to-day. In this process, it is important to identify only the red flags that are relevant to your business and to be as specific and thorough as possible. Be sure to consider:

- Previous incidents of identity theft that your institution has experienced. How did these occur and what warning signs could you have watched for to prevent the theft from happening?
- Sources of red flags. Where should you be looking to find the latest sources of threat?
- The most up-to-date methods of ID theft. What techniques are thieves using to steal identities in your industry today?
- The kinds of ID theft clues your current data security measuring tool cannot detect. Your data security tools can protect sensitive information, but what should you be looking for to stop ID theft once this data is already in their hands?

Use the following checklist to determine which common red flags your business may experience. If the red flag listed is something that could feasibly occur at your institution given your daily activity, or it is something you have experienced often in the past, check the "High Risk" box. If the red flag listed is something you could potentially run across but has not happened at your business before, check the "Risk" box. If the red flag listed is something neither you nor your employees would ever be exposed to because it is not within the nature or scope of your business, check the "N/A" box. When it is complete, take the list of possible red flags and use them as the foundation for your written Red Flag Rule Program. Place extra focus and attention on the "High Risk" red flags. Remember that the more specific you are in identifying possible red flags, the more complete your program will be. Larger institutions and those at a higher risk for experiencing the warning signs of identity theft should perform a much more complete and industry specific analysis of red flag risks that goes far beyond the checklist presented below.

Red Flag	High Risk	Risk	N/A
Alerts, Notifications and/or Warnings from a Credit Reporting Company, such as:			
1. A fraud or active duty alert on a credit report	☐	☐	☐
2. A notice of credit freeze in response to a request for a credit report	☐	☐	☐
3. A notice of address discrepancy provided by a credit reporting agency	☐	☐	☐
4. A credit report indicating a pattern of activity inconsistent with the person's history	☐	☐	☐
Suspicious Documents, such as:			
1. ID that looks altered or forged	☐	☐	☐
2. The person presenting the ID doesn't look like the photo or match the physical description	☐	☐	☐
3. Information on the ID differs from what the person presenting the ID tells you or doesn't match other information, like a signature card or recent check	☐	☐	☐
4. An application that looks like it's been altered, forged or torn up and reassembled	☐	☐	☐

Understanding and Preventing Data Breaches

What do Target, Nieman Marcus and Apple have in common? All these companies were victims of a data breach in 2013, totaling millions of stolen records that include personal information such as Social Security numbers, credit card numbers and bank account numbers.

If your company handles critical assets such as customers' personal data, intellectual property or proprietary corporate data, you are at risk of a data breach. It doesn't matter if you are a Fortune 500 company or a small "ma and pa" shop—cyber thieves are always looking for their next score. It is often assumed that smaller businesses can escape attention from cyber crooks, but according to Verizon Communication's 2013 Data Breach Investigations Report, 31 percent of data breaches were at companies with 100 or fewer employees. No company of any size is completely safe from a data breach.

Data Breach Basics
A data breach is an incident where private data is accessed and/or stolen by an unauthorized individual. Data can be stolen by a third party, such as a hacker, or by an internal actor (perhaps a disgruntled or recently fired employee).

According to the Ponemon Institute's Cost of Data Breach Survey, the average per record cost of a data breach was $201 in 2013, and the average organizational cost of a data breach was $5.9 million.

Data Breach Prevention Techniques
To reduce the chance for a data breach, it is wise to develop an IT risk management plan at your organization. Risk management solutions should leverage industry standards and best practices to assess hazards from unauthorized access, use, disclosure, disruption, modification or destruction of your organization's information systems. Consider the following when implementing risk management strategies at your organization:

- Create a formal, documented risk management plan that addresses the scope, roles, responsibilities, compliance criteria and methodology for performing cyber risk assessments. This plan should include a description of all systems used at the organization based on their function, the data stored and processed and importance to the organization.
- Review the cyber risk plan on an annual basis and update it whenever there are significant changes to your information systems, the facilities where systems are stored or other conditions that may affect the impact of risk to the organization.

Not all companies have the resources to create and implement a fully customized plan. However, there are many simple, cost-effective steps any business can take to help prevent a data breach.

- Never give sensitive information like Social Security numbers or credit card numbers out over the phone unless you can verify the identity of the person on the other line.
- Shred all credit reports and other sensitive data before disposal.
- Educate employees about phishing and pharming scams. Remind them not to click on anything that looks suspicious or seems too good to be true.
- If your company doesn't have an IT department, hire an outside company to set up the proper security measures for your computer network.
- Always monitor credit reports and other financial

data for the company. If you see things that don't belong, investigate.

Do not allow employees to write down passwords in the office.

Always encrypt sensitive data.

What to Do if You Have a Data Breach
It is common to have an "it will never happen to us" philosophy when it comes to data breaches. Unfortunately, that thinking can lead to lax security measures and carelessness when it comes to protecting sensitive information. If your company suffers a data breach:

1. **Act quickly**. Report the breach immediately to local law enforcement. Notify important suppliers, vendors and partners.
2. **Alert your customers**. If there is a data breach involving customers' personal information, activate your plan to alert them. The information compromised could be incredibly harmful to your customers, so alert them as soon as possible.
3. **Investigate**. If you do not have the resources to do an internal investigation, consult a third party. The quicker the breach can be dealt with, the fewer negative effects your company will endure.
4. **Take measures to lessen the chance of a future breach**. Fortunately, a data breach can be a good learning tool for your company. Analyze why the breach happened and take steps to make sure it doesn't happen again.

The Federal Trade Commission (FTC) has many resources available to assist you and your company in recovering from a data breach. Those resources can be found on the FTC's website: http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html

Insurance is Important
Chances are, your company doesn't have a "rainy day fund" capable of paying for data breach remediation. Fortunately, there are insurance options available to make recovery easier.

Cyber liability insurance policies can cover the cost of notifying customers and replace lost income as a result of a data breach. In addition, policies can cover legal defense fees a business may be required to pay as a result of the breach.

It's important to remember that it is cheaper to prevent a data breach by securing data than it is to lose that data from a breach. A data breach insurance policy can give you peace of mind and allow you to allocate resources to help keep data secure.

We're Here to Help
A data breach can be very costly and even has the ability to shut a business down. Contact Bankers Insurance, LLC today for resources to help support your cyber security efforts. We have the expertise to ensure you have the right coverage in place to protect your business from a data breach.

Protect Yourself Against Illegal Acts with Crime Coverage

You may feel that your employees would never steal from you or that your business would never be the victim of theft, but the harsh reality is that nearly every business is eventually victimized by fraud or theft. In this day and age, thieves (and potentially your employees) do not need direct access to cash to steal from you; merchandise, supplies and securities are all fair game. You may also be susceptible to losses in the event that finished products or even raw materials are stolen right from under your nose. Essentially, any product can be a target for thieves if there is an opportunity to make a resale profit.

The following examples represent common business thefts, specifically by employees:

- Keeping two sets of books
- Stealing from the cash drawer
- Stealing merchandise and materials
- Charging inactive accounts
- Paying bonuses to those that are not supposed to receive them
- Increasing amounts on checks and invoices after they have been paid
- Paying bills to companies that do not exist and then cashing those checks
- Reducing the amounts of outgoing invoices in the books, then paying the reduced amount in cash and then appropriating the customer's check
- Padding payroll and cash expenditures
- Not crediting cash payments
- Removing ledger sheets from the business to cover up shortages
- Invoicing materials below sale price and receiving the undercharge from the customer
- Issuing checks for goods that were not returned
- Stealing incoming payments and applying that money to subsequent remittances

Insurance Solutions to Combat Theft

Here are some policies that can safeguard your business against theft:

- **Employee theft coverage** protects your money and your business against theft, both from inside the organization and out.

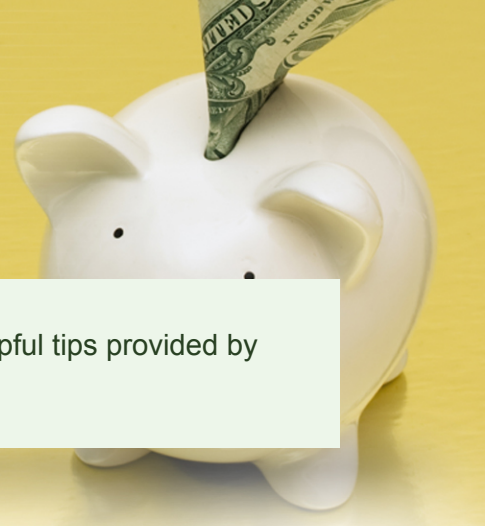
Protect Yourself Against Illegal Acts with Crime Coverage

- **Depositors forgery or alteration coverage** protects against losses by forgery or alterations of checks, drafts, promissory notes, orders or directions to pay money that is drawn upon you or is drawn upon your accounts by someone acting as your agent.
    - Also protects against forgery losses inflicted by people other than employees
- **Theft disappearance and destruction coverage** protects against loss of money and securities by way of theft, disappearance or destruction while the property is on your business and/or banking premises.
    - Protects against losses as a result of attempted or actual robberies while the property was on your premises
    - Protects against loss to other property in a safe or vault from an attempted or actual robbery within your premises
    - Outside of your premises, coverage protects money, securities and other property in the care of a messenger
    - Covers losses inflicted by those other than employees
- **Robbery and safe burglary coverage** protects against loss of money or securities on your premises, or while in the custody of a messenger outside of your premises.
- **Computer and funds transfer fraud coverage** protects against loss of money, securities and other property via computer fraud.
    - Covers money that that is directly related to the use of a computer to fraudulently cause a transfer of property from your premises or banking premises to someone or some entity outside of your premises
    - Pays for the loss of money through fund transfers communicated to a financial institution
- **Money orders and counterfeit currency coverage** protects against losses that are not paid upon presentation or are in the form of counterfeit United States and Canadian currency paid in exchange for goods or services.
- **Public employee theft coverage per loss** protects your money, securities and other property when it is stolen by employees. The maximum recovery for a single loss is outlined in your insurance policy, regardless of how many employees were involved in the theft.
- **Public employee theft coverage per employee** protects your money, securities and other property when it is stolen by employees. The maximum recovery for a single or multiple losses is outlined in your insurance policy, and applies to each employee involved.

Other Safeguards Against Theft

In addition to purchasing insurance protection against theft, consider implementing these safeguards in your business:

- Secure raw materials, semi-finished goods and finished goods in walled, fenced or locked areas on your premises.



PLAYING IT
SAFE

Be safe and healthy on the job at with these helpful tips provided by Bankers Insurance, LLC

Keeping Cash and Customers Safe

Helpful tips for bank employees

The large amount of cash that banks deal with each day creates a significant amount of risk. How you handle cash while on the job can help reduce the chance for a monetary loss. Even more importantly, how you handle yourself during a hold-up situation can prevent injury or death.

Cash Drawers
When using a cash drawer:

- Open it only when making a transaction.
- Close the drawer before you turn your attention away to other duties.
- When a customer is making a deposit, always count out the money they give you in front of them to verify the amount.
- When a customer is making a withdrawal, count out the money you are giving to them aloud.
- Never leave an open cash drawer unattended for any length of time.
- Notify your supervisor when you build up excess cash in your drawer so it can be moved to a more secure location.
- Never count cash drawers in front of customers. Always count the contents of the drawer in a secure, private area.
- Always lock the cash drawer and remove the key when it is not in use.
- If the premises will be unattended overnight, empty the cash drawer and leave it open to deter damage in the event of a break-in.

Hold-Ups
Even when employees take all the proper precautions, there is still chance for a robbery. If a robbery occurs while you are at work, remember to:

- Remain as calm as possible. This will go a long way in keeping others around you, and the robber, calm.
- Comply with the robber's instructions.
- Announce your actions to the robber so they are not threatened by your movements.
- Give them any money or goods that they ask for without resistance, but do not offer up other things they have not mentioned.
- Make mental notes about the robber's appearance so you can inform police.
- Never attempt to physically stop an armed robber.
- When the robber leaves, secure the building as soon as it is safely possible.

Do what you can to make sure you stay safe during a dangerous situation – do not try to be a hero. Your first priority should be to make sure everyone on the premises remains safe by trying to bring the situation to an end as quickly as possible.

Stay Calm, Don't Panic

If a robbery occurs while you are at work, try to remain calm and comply with the robber's demands. The most important thing is that people remain safe and that the situation ends quickly. Never try to stop a robbery. Money can be replaced, but your life can't.

safety matters

Financial Institutions Toolbox Talks for

From your safety partners at Bankers Insurance, LLC

Safety Tips to Prevent Accidents

You may not consider your job to be hazardous, but accidents can happen when you least expect them. However, many on-the-job accidents can be avoided by focusing on safe practices and taking necessary precautions.

Most accidents are caused by an unsafe act, an unsafe working condition or a combination of the two. For example, a worker can sustain a back injury while lifting a heavy box—an accident caused by the unsafe act of lifting an object that was too heavy. Or, a spill on the floor could cause someone to fall, and that would be the result of an unsafe condition. But, that unsafe condition was caused by the unsafe act of not cleaning the spill. In either instance, the accident could have been prevented by following proper safety precautions.

Hazards You May Encounter

Though safety is probably not a top concern in your daily activities, it is important to consider potential sources of accidents so that you can avoid them whenever possible. While it is impossible to list all of the hazards you may encounter while working, common ones include:

- Injuries caused by spills or debris on the floor
- Damaged equipment or facilities
- Damaged electrical cords or wiring
- Injuries caused by improper lifting techniques or improper use of equipment
- Accidents caused by unpredictable customer behavior
- Horseplay

Safe Steps to Avoid Accidents

The first step to keeping yourself and co-workers safe is to stay alert on the job and don't let routine or familiarity lure you into carelessness. Always observe safety precautions before and during a task, even if the task seems like a simple one. This includes cleaning up after a task—items left where someone could trip on them or that are improperly stored can cause an accident.

Next, know your job and your workplace. Be aware of any safety precautions for tasks you perform, and be on the lookout for safety hazards around the office. Even a task as routine as making coffee could be hazardous if the cord is damaged or the machine malfunctions. Also, be aware of customers or clients in the building. If you see a customer behaving unsafely or committing an unsafe act, inform the customer and explain how to safely correct his/her behavior.

And finally, make a personal contribution. A good way to start this is to follow all safety rules, even if you think they are unnecessary or slow you down. Certain rules in the workplace are made for your protection, so follow them. In an environment that many don't consider dangerous, the most important action is to be alert for any unsafe conditions and to fix or report them immediately.

It's important to always stay alert for any unsafe conditions and to fix or report them immediately.