At Assurant, we pride ourselves on our ability to help our clients and customers reduce their exposure to risk. We have a commitment and a responsibility to protect the confidential information that has been entrusted to us.

Across the globe, we've built our reputation on offering peace of mind to the businesses and communities we serve. That's why it's so important to protect the information that passes through our hands each day. This brochure contains guidance to help you maintain our reputation by caring for information as though it were your own.

Physical Security

- Always wear your company badge.
- Report a lost or stolen ID badge immediately.
- Don't allow someone to follow you into secure areas without authentication — this is tailgating.
- Be aware of your surroundings.
- Notify Security or your manager of any suspicious activity.

Printed Paper Information

- Don't print Restricted information
- Always keep printed Confidential information in a secure place. Whenever possible, lock file cabinets and desk drawers when leaving your workspace.
- Limit access to Restricted & Confidential information — only those with a business "need to know" should have access.
- Always retrieve copies, faxes, and printouts immediately and at the end of your workday.
- Understand and follow Assurant's Clean Desk Policy available in the Assurant Employee Handbook.
- Don't fax Restricted information. Don't fax Confidential or Restricted information to a public fax machine or recipient unless you know the individual is permitted to retrieve it.
- Don't publicly display Confidential or Restricted printed materials.

Records & Information Management

- Read, understand, and follow Assurant's RIM policy for the proper handling and life cycle of business records.
- Review electronic files on a regular basis and purge them after the appropriate retention time.
- Properly dispose of records according to the Privacy Policy. Examples of Assurant's classification of information are outlined in the table below.

DATA CLASSIFICATION	
RESTRICTED	
• Customer or client personal information (PII): name, address, Social Insurance or Security number, date of birth	• Credit card numbers • Passwords/credentials • Health/medical records • Credit reports
CONFIDENTIAL	
• Customer Financial Records • Business Contracts	• Client Information, Customer Lists, Relationship Data • Intellectual Property
INTERNAL USE	
• General Business Documents	• Company Policies and Procedures
PUBLIC	
• Marketing Campaigns • Stock Price	• Earnings Statements

Resources & Contacts

- Information Security: ITSecurity@Assurant.com
- Website: AssurantConnects.SharePoint.com/Teams/Compliance/Information-Risk-Compliance-Office/
- Privacy Office: ThePrivacyOffice@assurant.com
- Help Desk: 1-800-554-6386

ASSURANT®

AIZ-14981-1122

ASSURANT®

KEEP INFORMATION SAFE AND SECURE

Employee Quick Guide

PRIVACY & SECURITY TIPS

General Information

- Read and follow Assurant's policies, located on Connect.
- Read and understand the privacy notice(s) that are distributed to our customers, clients, and claimants.
- In additional to adhering to the classification requirements, treat all customer/client information with the highest degree of confidentiality.
- Never share Restricted or Confidential information about a customer, client, claimant, or employee without the appropriate authorization or permission.
- Always report a suspected or real loss of Restricted or Confidential Information to the Privacy Office.
- Exercise extreme care when handling Restricted information.
- Remember: All our actions and inactions are highly regulated.

Social Engineering

- To help prevent social engineering, identify callers before giving out any information.
- Beware of emails requesting confidential information, credit card number, or bank account information.

Electronic Information

- Storage of Restricted, Confidential and Internal Use data on a local drive ("C" drive) is limited to proper business content.
- Restricted, Confidential and Internal Use information must only be stored on encrypted portable devices and storage media.
- Computer and application access is limited to only the information that's required to perform your job function.
- Access privileges are reviewed by data owners, corporate security teams, and management on a periodic basis.

Avoiding Malicious Software & Viruses

- Beware of opening attachments in emails from individuals or email addresses that you don't recognize.
- If you get a virus alert on your computer, contact the Help Desk immediately!

Verbal Information

- Be aware of where you are and who is listening. Don't discuss confidential company business in public places.
- Don't provide a caller with a Social Insurance Number, credit card details, or any other Confidential personal information.

Social Media

- You're personally and legally responsible for the content you publish, so always pause and think about the potential consequences before posting.
- Don't disclose any Restricted, Confidential or Internal Use information.
- Don't use social media for business purposes unless you are authorized by your manager or approved to fulfill your job duties.

Email/Internet

- Don't use internet email accounts such as Yahoo and Google to conduct Assurant business.
- Company internet and email are permitted for business use only.
- Be diligent and inspect incoming email from unknown senders. Attachments and web links may contain malicious software.
- Distribution or forwarding chain letters or personal messages for mass distribution isn't permitted.
- Assurant supports options to force email security and encrypting messages and attachments.
- Confidential emails should be sent securely. Restricted emails should be sent encrypted outside of Assurant using subject line tags.

To Manually Secure Email

Add **[Secure]** or **[Confidential]** in the subject line.

To Manually Encrypt Email Content

Add **[ppencrypt]** in the subject line.

Software Usage

- Use only Assurant approved and installed software. Use of personal software is not permitted.
- Don't download apps or share software without IT approval.
- Don't download games or free web software on company equipment.

Equipment

- Report lost or stolen equipment immediately to the Help desk at 1-800-554-6386.
- Company-issued equipment is the property of Assurant and used for business proposes only.
- Laptops must be stored securely or reside with you when the workday ends.
- Don't leave laptops in your vehicle.
- Never disable antivirus or company security software.