INFORMATION GOVERNANCE:

STRATEGIES FOR PRIVACY AND SECURITY COMPLIANCE

PRESENTED BY:

Anne Peterson
Counsel
Data Privacy and Security Practice Group
McGuireWoods, LLP

Dennis Smith
Privacy and Cybersecurity Counsel,
Senior Regulatory Counsel and
Senior Vice President
Citizens Financial Group, Inc.

October 10, 2019

McGUIREWOODS

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Agenda

1. Privacy and Cybersecurity
2. Trends in Privacy, Cybersecurity and Information Governance
3. Information Governance Strategies
4. Information Governance Compliance Framework

Privacy vs. Security

- **Privacy**
  - *The right to be let alone.* Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890)
  - *The right of individuals to control, edit manage and delete information about themselves and to decide when, how and to what extent information is communicated to others.* Alan Westin (1967)
  - *You have to realize that we're people and that we need, we just need privacy and we need our respect, and those are things that you have to have as a human being.* Britney Spears, 15 June 2006, NBC Dateline
- **Security**
  - Protection against unauthorized access to, and use of, information
  - Technical mechanisms that determine access and control
  - Security defines which privacy choices can be accomplished

3

Compliance Framework – U.S.

State Regulation of Personal Information

- All states require notification to potentially affected individuals in the event of a data breach
- Definition of reportable data breach different in every state
- Personal information defined differently in every state
- California, New York, Massachusetts and Colorado require data identification, cybersecurity safeguards, incident response
- 28 states require "reasonable security" measures to protect information
- "Highest Standard" compliance

Federal Regulation

- HIPAA
- Gramm-Leach-Bliley Act
- Securities and Exchange Commission Guidelines
- Federal Trade Commission Guidelines

Industry Standards

- Payment Card Industry/Data Security Standards (PCI/DSS)
- NIST Cybersecurity/(Proposed) Privacy Frameworks
- ISO 27001/27002

4

Global Compliance Framework

EU General Data Protection Regulation ("GDPR")

Territorial Scope

- Includes U.S. companies if they:
  - have an establishment in EU
  - offer goods or services to EU Data Subjects
  - monitor behavior of EU Data Subjects in EU

Personal Data

- Name
- Job title
- E-mail address
- Business communications
- Location information
- Government ID

- Employee, customer, individual personal data
- Consent requirements for direct email marketing, processing of criminal information
- Data mapping and register of processing activities fundamental to compliance
- Legitimate bases for processing must be documented
- Internal/External Privacy Notices
- Procedures for Data Subject Access Requests
- Risk Assessments

5

How Information Governance Became Corporate Governance

- C-level and Board Exposure
- Internet/Social Media and Marketing
- Increased Legal and Regulatory Requirements
- Cybersecurity Risks
- Big Data/Operational Requirements
- Mergers/Acquisitions/Divestitures
- E-Discovery
- Industry Standards – especially PCI/DSS

The goal of information governance is to ensure relevant, trustworthy information on demand without violating legal requirements and risk thresholds.

6

Why Information Governance Will Remain Corporate Governance

- *C-level and Board Exposure*
- July, 2019, Facebook record setting *$5 billion* settlement with FTC
- Result of investigations into Cambridge Analytica and other privacy scandals
- Facebook violated the law by:
  - *Failing to protect individual profile data from third parties*
  - *Serving ads through the use of phone numbers provided for security*
  - *Claiming that the facial recognition software was turned off by default*
- In addition to imposing the fine, the FTC requires:
  - *Facebook to conduct privacy reviews for all new products/services*
  - *CEO and a third party to conduct privacy reviews every quarter*

FTC: "The Order imposes a privacy regime that includes a new corporate governance structure, with corporate and individual accountability and more rigorous compliance monitoring. . ."

7

Why Information Governance Will Remain Corporate Governance

- *Facebook Settlement Requirements and Implications for Corporate Governance:*
  - Board-level privacy committee for greater accountability at highest level
  - Members of privacy committee must be independent (officers and employees disqualified from membership)
  - Members appointed by independent nominating committee
  - Removal of privacy board members only by supermajority of the Facebook board of directors
  - The privacy committee must be informed about all material privacy risks and issues
  - Designation of "expert" compliance officers approved by the independent privacy committee
  - Compliance officers responsible for implementing and maintaining privacy program and documenting material privacy decisions
  - Third- party assessor review of compliance officers' documentation and quarterly certification to FTC regarding status of compliance with privacy program

Facebook settlement provides guidance as to additional privacy governance structure. But which business area should own the program? Legal, Risk, Compliance, IT? How should the independence of key positions (CISO/DPO) be protected? Reporting lines?

8

Corporate Perspectives

- Information is our most valuable asset, ***BUT***
- Lack of data control leads to data ***in***security
  - What data do we have?
  - Where should it live in the corporation?
  - How do we use/share/sell it?
  - How sensitive is it?
  - How vulnerable is it?
  - What are the threats?
  - What do we do if we're breached?
  - What's our liability exposure/contractual safeguards?

If you don't know your information, you cannot protect against:

- ***Theft of IP***
- ***Loss of competitive edge***
- ***Data breaches / inadequate response***
- ***Legal noncompliance (privacy and security)***
- ***Agency enforcement actions***
- ***Litigation - Customer/Shareholder/Business Partners***
- ***Reputational damage***

9

Risk Factors

- **Operational Risk Factors**
  - Lack of cost-efficient, centralized privacy/security program
  - Poor crisis management
  - Inadequate vendor/third party management
- **Legal Risk Factors**
  - Increased SEC/state/foreign scrutiny
  - Aggressive enforcement actions/class actions
  - Diverse, complex regulatory compliance obligations
- **Cyber Risk Factors**
  - Customer and market sensitive data
  - Valuable "know how" and trade secrets
  - Hackers/state actors/insider threats
  - Reputation

10

Risk Mitigation Alert: Training = Compliance

GDPR

- Art. 39 – " awareness-raising and training of staff involved in processing operation."
- Art. 47 - "the appropriate data protection training [for] personnel having permanent or regular access to personal data."

CCPA

- Section 1798.130(a)(6) – "individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance. . ."
- All individuals responsible for handling consumer inquiries about company's privacy practices
- All individuals responsible for the CCPA compliance

- In 2018 alone, about 4.5 billion records were exposed as a result of data breaches.*
- The average cost of a data breach is $3.86 million*
- Hackers are no match for human error – human error is responsible for 47% of data breach events**
- 50% of Internet users receive at least one phishing email a day***
- 97% of the people in the world cannot identify a phishing email***
- One in 25 individuals actually clicks on phishing emails***

*IBM 2019

**CNBC, *The biggest cybersecurity risk to US businesses is employee negligence*, June 21, 2018.

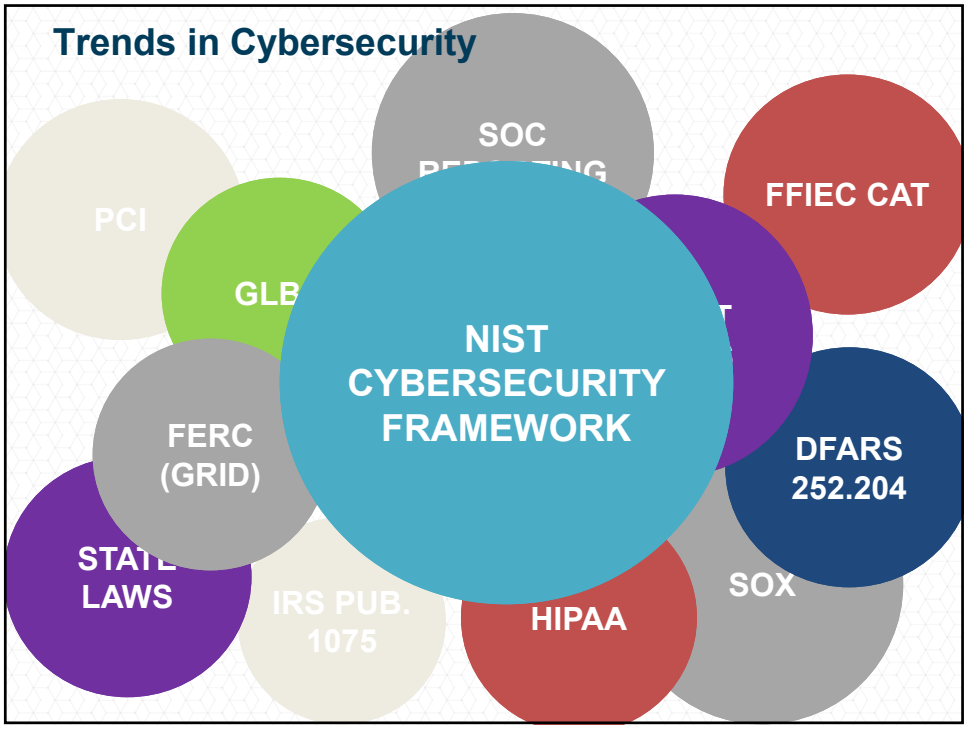
*** Infosec, *Is Security Awareness Important?*, retrieved at https://resources .infosecinstitute.com/category/enterprise/securityawareness/security-awareness-fundamentals/security-awareness-statistics/#gref

11

Trends in Cybersecurity

Evolving Attack Vectors:
Social Engineering/Phishing
Poor Vendor Management
Mobile Devices
Ransomware
Social Media
Malware
Human Error

12



IG Challenges/Strategies/Benefits

CHALLENGES

- Obsolete, Non-Compliant and/or Inconsistent Information Management Policies, Procedures and Practices
- Numerous Jurisdictions and Global locations
- Sensitive, Regulated Information in Distributed Systems
- PCI/DSS Compliance
- Non-compliant Cross-Border Data Transfer
- No Written Information Security Policy and/or Data Breach Response Plan
- Inconsistent/Unknown Vendor/Third Party Contract Terms for Data Privacy and Security
- Ad hoc Legal Hold and E-discovery Processes
- Limited Business Intelligence for Targeted Marketing

BENEFITS

- Fast and Accurate Business Intelligence
- Legal and Industry Standard Compliance
- Safe and Secure Data
- Reduced Costs and Effective Risk Management for Litigation
- Leverage Information for Marketing Purposes

STRATEGIES

- Map Sensitive and Regulated Information
- Implement Consolidated, Defensible Information Management, Data Privacy and Security Policies, Procedures
- Build in Jurisdictional Requirements
- Document Safeguards and Identify Gaps in Security
- Map PCI/DSS requirements to Policies and Procedures
- Defensible Cross-border Data Transfer
- Vendor Management/Monitoring/Audit
- Consistent and Cost-Effective Legal Hold and E-discovery Processes
- Compliant/Effective Marketing

Defensible Information Governance Building Blocks

1. **Information Inventory/Data Map**
   (*Priority* Regulated/Sensitive Data, Information Location & Format)
2. **Global Retention Schedules**
3. **Policies and Procedures**
4. **Training**
5. **Audit/Corrective Actions**
6. **Defensible Destruction**

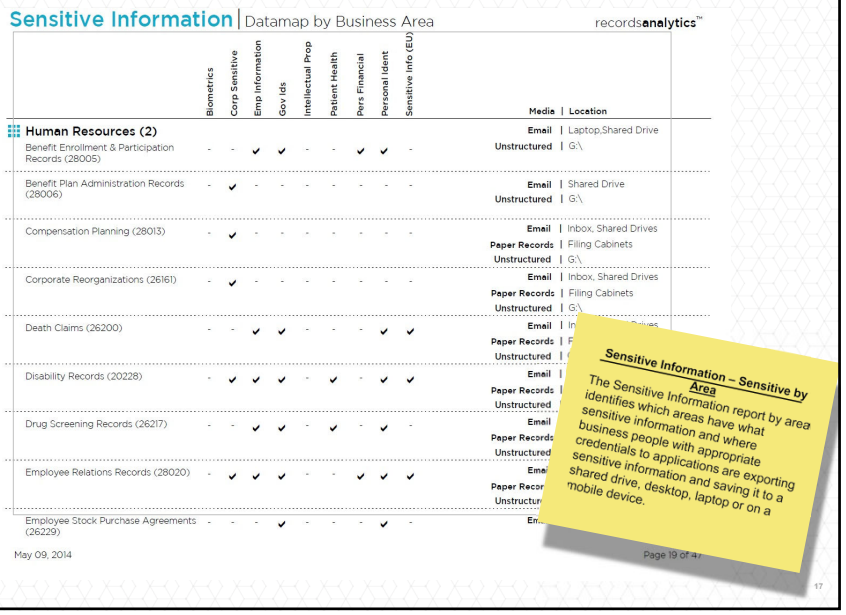
15

Information Governance Framework

Information and Records Management Policy	Global Records Retention Schedule	Information Classification and Destruction Policy
Backup & Disaster Recovery Policy	Privacy Policies/Notices	Written Information Security Policy
BYOD/E-Comm/Acceptable Use/Social Media Policies	Legal Hold Procedures and Forms	GDPR /CCPA Policies
Risk Assessments	Global Incident Response Plan	Training

16

Sensitive Information – Datamap



Reporting Formats

Project Reports
Participants by Role
Status Report

Retention Reports
Best Practice Variances
Over-Retention
Retention by Authority
Retention by Business Area
Under-Retention

Record Type Reports
Data Classification
Discovery Datamap
Email Datamap
Master List
Multiple Official Owners
No Official Owner
Paper Datamap
Regulatory Tags
Shared Drive Datamap
Structured Content Datamap
Unstructured Content Datamap

Sensitive Information Reports
Areas Using Mobile Devices
Data Subjects
Datamap by Application
Datamap by Business Area
Datamap on Mobile Devices
Datamap by Record Type
Distribution to Personal Email Accounts
Identified by Application
Record Types on Mobile Devices
Retention Variances to Best Practice
Sensitive Info Area Overview
Sensitive Record Type Overview
Sensitive Tags by Area
SME Cyber Insurance
Snapshot of PII

Movement Reports
Enterprise Application Extraction

Statistical Reports
Business Area Snapshot
Offsite Storage
Record Type Distribution
Shared Drive Distribution by Area

Subject Matter Expert (SME) Reports
Access Control
Business Continuity Management
Desktop Administration
Email Administration
Email Backup
File Server Administration
File Server Backup
Human Resources
InfoSec & Compliance
InfoSec Incident Management
InfoSys Acquisition Maintenance
Litigation Readiness
Offsite Records
Organization of InfoSec
Physical & Environmental Security
Program Manager
SharePoint
Storage / Virtual Backup

Global Retention Schedule

PRIVILEGED AND CONFIDENTIAL
RECORDS RETENTION SCHEDULE

Business Area	Record Type	Records Description/ Examples	Retention Period (all periods in years unless otherwise noted)	Information Classification	Format/ Location	Legal Authority/ Substantive Comments	Operational Requirements
Accounting, Finance & Tax							
Accounting	**Accounts Payable/Receivable Records**	Accounts Payable Reconciliations, Accounts Payable Vouchers, Check Requests, Employee Travel and Expense Reports, Invoices, Monthly Vouchers, Overpayment/Refund Check Records, Payment Authorizations, Vendor Payments, Accounts Receivable/Payable Ledgers and Aging, Billing Records, Cash Receipts, Customer Invoices, Insurance Premiums,	10	Internal Use		Retention period based on SL and tax considerations.	
Accounting	**Account Reconciliation Records**	Balance Sheet Reconciliation, Spreadsheets, Reports, and Related Records	10	Confidential		Retention period based on SL and tax considerations.	
Finance	**Annual Reports**	Company Annual Report containing Financial Statements	PERM	Public		Retention period based on best practice considerations. IRCH recommends a Permanent retention of Annual Reports.	
Accounting	**Bad Debt and Collections Records**	Collections Report, Process Materials, Delinquency Correspondence, Delinquency Summary Reports, Uncollectible Account Information, Write-Off Documentation, Workout Documentation	ACT + 10 *ACT means until the account is closed	Confidential		Retention period based on SL and tax considerations.	
Accounting	**Banking Records**	Bank Reconciliations, Bank Statements, Bank Deposit Slips, Cancelled Checks	10	Internal Use		Retention period based on SL and tax considerations.	
Finance	**Budgets and Financial Forecasts**	Budget Forecasts, Budget Preparation and Planning Records, Budget Records and Reports, Financial Planning Records, Forecasting Materials, , Loss Ratio Analysis, Operating Budgets	No legally required retention period. Retention subject to business discretion.	Confidential		N/A	

Data Map By Business Process

ACTIVE SYSTEMS

BUSINESS PROCESS	APPLICATION/LOCATION	SERVER LOCATION
ACCOUNTING	CASH AUDIT / GL / NEXT DAY LEDGER/MAG/DB2	NT01/PITTSBURGH, PA
	MAINFRAME INTEGRATION/MOT	WWW.INTEGRATE.COM/ SAN FRANCISCO, CA
	SERVICING OUTSOURCING/MSO	WWW.MSA.COM/N.Y. NY
CROSS-FUNCTIONAL	MAIL CENTER/MCT	NT02/PITTSBURGH, PA
	EQUIPMENT TRACKING/ETS	NT02/PITTSBURGH, PA
POST-CLOSING	WINCMSS/MCW/DB2	
	IMAGE EXPRESS/IMZ/SQL SERVER/ORACLE	
	DOC TRACKER/DTR/DB2	
	VIRTUAL CORPORATE KEEPER/VCK	
	RECORDS MASTER/IMZ/DB2	
REPORTING - ACCOUNTING	DATAMART/DTN/DB2	
	DCIE/OCE/DB2	
REPORTING - CREDIT RISK	CREDIT RISK ANALYTICS/SAS/SAS (HOSTED OR OUTSOURCED?)	
REPORTING - CROSS-FUNCTIONAL	BRO/DBR	
	MORTGAGE DATA WAREHOUSE/MDB/ORACLE	
REPORTING - FINANCE	ESSBASE/EBM/ESSBASE	
REPORTING - OPERATIONS POST-CLOSING	CDS/MODATART/CSL/DB2	
REPORTING - SALES/OPERATIONS	RETAIL ANALYSIS/RAN/SQL SERVER	
	PRICING DATABASE/PDB/SQL SERVER	
REPORTING - SERVICING	SERVICING DEFAULT REPOSITORY (AKA TDW)/SDR/SQL SERVER	
	INVESTOR REPORTING/ITR	
REPORTING - SERVICING REPORTING - ACCOUNTING	SERVICING DATA FEEDS/MSV/MLA	
RISK/QC/COMPLIANCE	RATA/SMT	
	ENTERPRISE CUSTOMER COMPLAINT SYSTEM (ECCS)/CCT/ORACLE	
	EVEREST/EVE	
	COGENT/CGT/CGS/SQL SERVER	
	CONDO WEB QUESTIONNAIRE/CWQ/SQL SERVER	
	LOAN REVIEW SYSTEM/LRS/SQL SERVER	

BUSINESS PROCESS	NAME OF APPLICATION/APPLICATION LOCATION/ DATABASE LOCATION	SERVER LOCATION
SALES	MOTIVATOR/SLS/DB2	
	GENESIS/GEN/DB2	
	CONSUMER DIRECT POS/MVS/SQL SERVER	
	CSC/CS/SQL SEVER	
SALES ORIGINATION	IMPACT (REPORTING)/LOS/ORACLE	
SALES OPERATIONS POST-CLOSING SERVICING	INTEGRATION HUB/MPH/ORACLE	
SECONDARY	PRICING EXPRESS/PDB/SEQUEL SERVER	
SECONDARY POST CLOSING	CRM/XQM/SQL SERVER	
SERVICING	PROCESS MANAGEMENT/DPM	
	PASSPORT/PSP	
	INVOICE MANAGER/DIM	
	VENTURE/PNT (PAPER ARCHIVES?)	
	FIDELITY CHECKPRINT/FCP	
	FIRST AMERICAN DOCS/FIR (PAPER ARCHIVES?)	
	SPEEDPAY/SPD	
	CASH TRANSFORM FORM/CTF/SQL SERVER	
	MORTGAGE LINK/MVC/CC	
	CUSTOMER CARE/NET/CCN	
	CSC EARLY RESOLUTION/ERZ	
	COMMERCE VELOCITY NPV TOOL/CVT	
	LOSS MITIGATION SITE/LMT/SQL SERVER (IS THIS NOW A LEGACY SYSTEM?)	
	XERS/XRE	
	VSI RELEASE/VSR/SQL SERVER	
	VSI ESCROW/VEA/SQL SERVER	
	DIRECTOR (N/A - MSP UPDATE TOOL)/DIR	
	MORTGAGE TRANSACTIONAL DATABASES/MTD/SQL SERVER	
	CMAX/MAX	
	LOAN SERVICING APPLICATION/LSA/ORACLE	
	ELI/ELI	

OUTSOURCED/HOSTED DATA

BUSINESS PROCESS	NAME OF APPLICATION/APPLICATION LOCATION/ DATABASE LOCATION	SERVER LOCATION
SALES	DORADO PARTNERLINK/ACB	
CROSS-FUNCTIONAL	DAPTIV/DPV	
SERVICING	MSP/MSP (ARE THE RELATED MSP MODULES, PSP, DIM, PNT, FCP, FIR, SPD ALSO HOSTED BY LPS?)	
POST-CLOSING	INVESTOR DELIVERY/LDS/GNN/SSF	
REPORTING - CREDIT RISK	CREDIT RISK ANALYTICS/SAS/SAS (REMOTELY HOSTED?)	

PAPER ARCHIVES

BUSINESS PROCESS	NAME OF APPLICATION/APPLICATION LOCATION/ DATABASE LOCATION	ARCHIVE LOCATION
POST-CLOSING	RECORDS MASTER OUTPUT	PHYSICAL DOCUMENTS THAT HAVE BEEN IMAGED IN IMZ RETAINED IN BINS 90+ DAYS/MIAMISBURG, PA (?)

LEGACY SYSTEMS

BUSINESS PROCESS	NAME OF APPLICATION/APPLICATION LOCATION/ DATABASE LOCATION	SERVER LOCATION/OTHER LOCATION
SERVICING	LOSS MITIGATION SITE/LMT/SQL SERVER (IS THIS NOW A LEGACY SYSTEM?)	

Written Information Security Policy

McGuireWoods LLP
Draft 6/30/16

PRIVILEGED AND CONFIDENTIAL

DRAFT

POLICY # Date of Issue: Date of Revision: *McGuire Woods Draft*	**Company** **Written Information Security Policy**
OVERVIEW	The objective this Written Information Security Program ("WISP") is to create effective administrative, technical, and physical safeguards for the protection of personal information of employees of Company and persons who do business with or otherwise interact with Company, in conformance with federal regulations and applicable state law. The standards defined herein are designed to minimize the potential exposure to Company from damages which may result from unauthorized use, disclosure and/or access to sensitive information. Potential damages include, but are not limited to, the loss of sensitive, personal and/or confidential data, intellectual property, damage to public image, and damage to critical Company computer resources and systems.
SCOPE	This Policy applies to all Company subsidiaries, affiliates, business units, departments, locations, and Company employees ("Employees"), as well as all contractors, consultants, temporary employees, and third-party service providers ("Third Parties") in all states where Company conducts business, ***unless and except where contrary to local laws***. This Policy governs Personal, Sensitive and Confidential Information as well as Company Computer Resources and Information Systems as more fully described below. ***Personal Information*** Personal Information is information that can be used on its own or with other information to identify a specific individual. This information identifies an individual, and includes a person's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public. ***Highly Sensitive Information / Confidential Use*** Highly Sensitive Information is information that, if compromised, could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means: (i) the company is not able to perform one or more of its primary functions; (ii) there is a major damage to organizational assets; (iii) there is a major financial loss; or (iv) there is danger of severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. Examples of High Sensitivity information include: Personally Identifiable Information ("PII"), Personal Health Information ("PHI"), attorney client privileged information, proprietary and company private information, personal financial

DRAFT

	Standards A. General Password Standards Passwords must be at least [INSERT COMPANY SPECIFIC POLICIES, PROCEDURES, PROCESSES] characters and a combination of upper- and lower-case letters, numbers and symbols. In addition, Employees and Third Parties should avoid passwords with the following characteristics: • The password is a word found in a dictionary (English or foreign); • The password is a common usage word such as: o Names of family, pets, friends, co-workers, fantasy characters, *etc.*; o Computer terms and names, commands, sites, companies, hardware, software; o The words "Company", "password" or any derivation; o Birthdays and other personal information such as addresses and phone numbers; o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, *etc.*; o Any of the above spelled backwards, and; o Any of the above preceded or followed by a digit (e.g., secret1, 1secret). B. Password Protection Standards [INSERT COMPANY SPECIFIC POLICIES, PROCEDURES, PROCESSES]
E-MAIL SECURITY PROCEDURES	Electronic mail (Email) and instant messaging have become ubiquitous services that greatly enhance communication, both internally within Company and externally. The ease of this form of communication results in the generation of large quantities of electronic information of various levels of importance to Company that is not quickly classified. All email containing Personal and Confidential information must be encrypted prior to transmission outside the Company network. Company has implemented automatic encryption procedures which are triggered when entering [ ] on the subject line of a specific email ***The encryption of sensitive and confidential information is mandatory when transmitting Personal and Confidential information outside the Company network.*** Please refer to the Company Acceptable Use and E-Communications Policy (#), and the Email Retention Policy #________ for more information regarding the classification of, and retention periods for, email.
HIGHLY SENSITIVE INFORMATION LOCATIONS	The below chart details the location of information that has been classified as Highly Sensitive Information, as defined in this WISP, and the governing regulations or internal requirements for security.

Platform / Repository	Type of Highly Sensitive Information	Applicable Regulation	Security [to be completed by Company]
	• Corporate Sensitive • Employee Information / Personally Identifying • Intellectual Property • Personal Financial	• 1974 Federal Employees Act*	
	• Confidential Donor Financial Information • Corporate Sensitive	• 1974 Federal Employees Act* • Graham-Leach-Bliley Act • Payment Card Industry Data	Blackbaud is a cloud based platform that tokenizes donor personal and financial

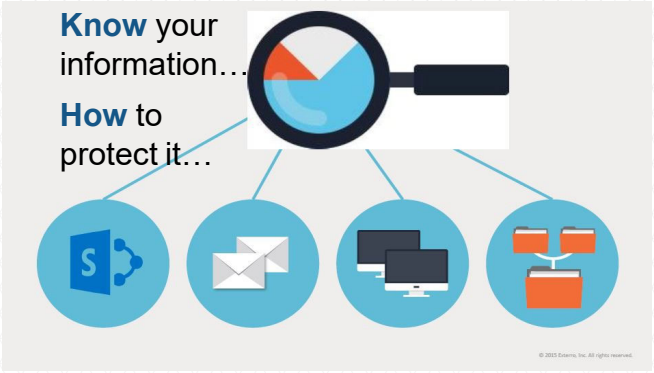
21

Training

- Information and Records Management
- E-Communications (Best Practices & Security)
- Legal Holds
- Data Security and Privacy
- Industry Specific Training (Government Contracts, Education, Manufacturing, Technology)

Onsite Training

End User Self Paced from Intranet



…and how to **maintain and grow value**.

23

Presenters

Anne S. Peterson | McGuireWoods LLP | Pittsburgh
aspeterson@mcguirewoods.com

Anne is Counsel in the McGuireWoods Data Privacy and Security practice group. Anne focuses on data privacy and security issues, incident response, information governance and vendor management. She routinely advises clients on a broad array of issues related to global, federal, state and industry compliance, as well as defensible policies and procedures to protect and leverage information. Anne is a Certified Information Privacy Professional (CIPP/US) and serves as a co-chair of the Pittsburgh International Association of Privacy Professionals (IAPP)/KnowledgeNet chapter, for which she leads privacy-related activities for more than 130 members. Anne is a former litigator and IBM Systems Engineer.

Dennis Smith | Citizens Financial Group | Richmond
Dennis.Smith@citizensbank.com

Dennis Smith is a Senior Vice President and Senior Regulatory Counsel at Citizens Financial Group. He primarily advises on various banking, securities, and corporate regulatory issues. Dennis also serves as Privacy and Cybersecurity Counsel for Citizens. Prior to joining Citizens, he was the Deputy General Counsel and the first Privacy Officer of the Federal Reserve Bank of Richmond. Dennis previously managed legal and regulatory issues for Wells Fargo & Company and SunTrust Banks, Inc.

24

Questions or Comments?