



Information Security Training

February 10, 2025

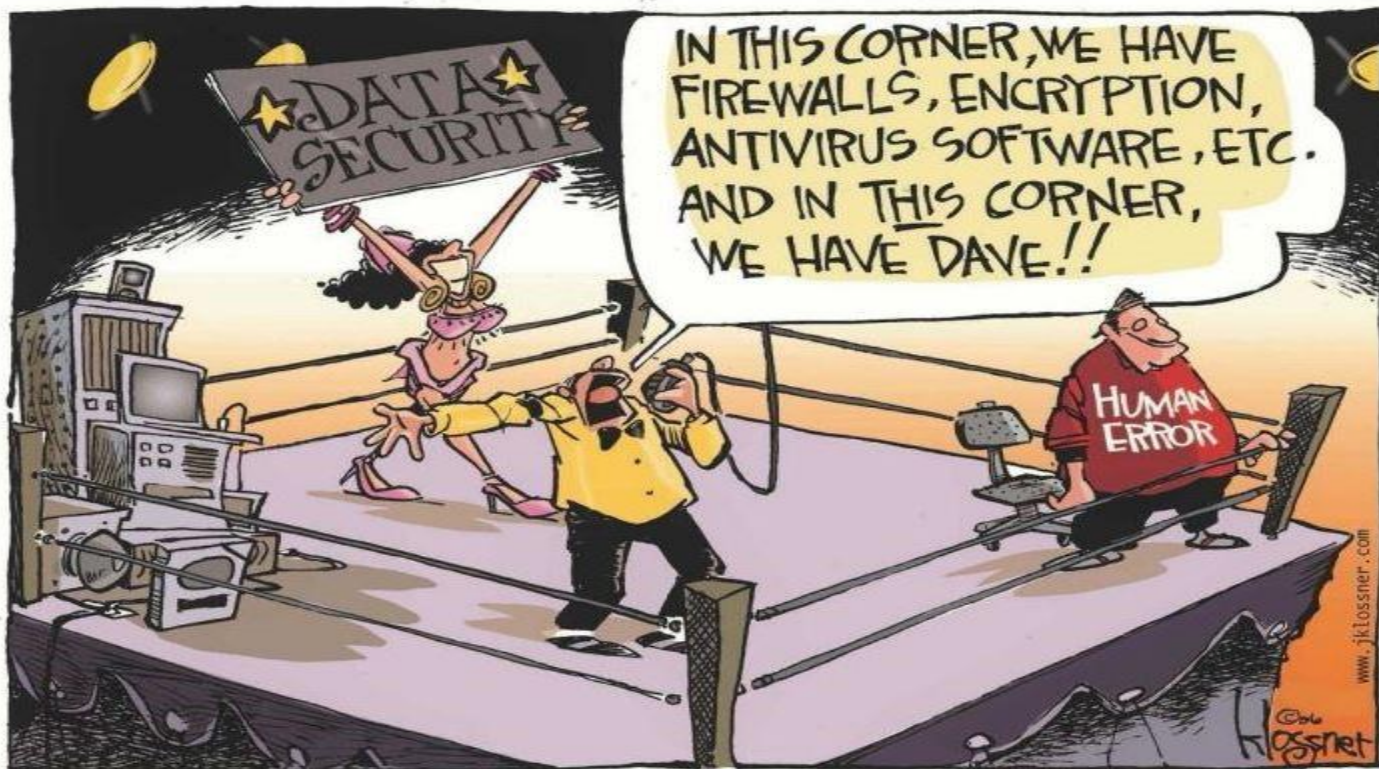


Agenda

- Why Do We Do Training?
- What is Personal Information? / Data Privacy
- General Data Protection Regulation (GDPR) – CHANGES
- Overview of our Written Information Security Plan
- Protecting Confidential/Sensitive Information
- “Passw0rds”, “P@ssw0rds!”, “P@\$sw0rd\$!”
- Email Phishing
- Overview of Procedures in the Event of a Breach.
- Business Continuity
- Anti-Fraud
- Cloud Storage
- Anti-Malware
- Compliance
- AI – Artificial Intelligence
- Anti-Harassment & Anti-Discrimination
- What’s Coming Next?
- Q & A

Why We Do Training?

**Employee negligence/ignorance
is the single biggest cause of data breaches**



Leading Cause of Breaches



Employees and the human element continue to be the weak link in the chain of data security. According to a BakerHostetler [report](#) drawing from over 200 incidents the law firm advised on in 2014, human error was the top cause of data security incidents, with employee negligence being involved 36% of the time.

Increasingly sophisticated technology helps, but does not eliminate security risk altogether. Organizations need to combine appropriate technical safeguards, employee training and awareness campaigns, and well-crafted information security policies and procedures to create comprehensive breach prevention programs.

The report also points out that it is important to remember that no organization is safe from threats to sensitive information, despite the industry or size.

What is Personally Identifiable Information (PII)?

**First Name or
First Initial**

PLUS

AND

Last Name

Any One of the Following:

- **Social Security #**
- **Driver's License #**
- **State-Issued I.D. Card #**
- **Credit Card #**
- **Debit Card #**
- **Financial Account #**

Privacy

Protecting Confidential/Sensitive Data

- Review specific types of personal and sensitive information that your department handles and examples of how it should be protected (e.g., redacting credit card numbers from email messages sent to customers)
- Confidential or Sensitive Information should only be disclosed when necessary for the business or job function. If the information is not needed, remove it.
 - External: Information we wouldn't want to tell our clients we lost
 - Internal: Information we wouldn't want to tell Foundation Source or GTCR we lost
- We are working on an improved **Data Classification Policy** and tech to enforce it (Timeframe for completion = TBA)

What Happens in the Event of a Breach?

- **STEP 1**: Immediately notify your manager, the CISO, CTO, or Director of IT Operations (Dan Schreck)
- **STEP 2**: The incident will be investigated and recorded by the security team – Foundation Source and GTCR will be notified
 - Expect to be part of the investigation
- **STEP 3**: If required, outside counsel and/or a forensics team will be engaged
- **STEP 4**: If warranted, authorities will be notified

Rapid Response is Critical

A quick response to an incident is important for several reasons, including:

- Creating the opportunity to stop an attack in its early stages before sensitive data is accessed,
- Preserving available forensic data to enable a precise determination of what occurred,
- Generating affirmative evidence to help the company respond in a way that protects affected individuals and minimizes potential financial and reputational consequences.

General Data Protection Regulation (GDPR) & California Privacy Rights Act (CPRA)



We **MUST** comply with Europe's GDPR and California's CPRA because donors can reside in the EU or California and are therefore covered by the GDPR or CPRA. **This is a change both from a legal interpretation perspective (GDPR) and us being part of Foundation Source (CPRA)!!**

If you are from the European Economic Area (EEA) or California, the legal basis for collecting and using the personal information described in this Privacy Policy depends on the Personal Data we collect and the specific context in which we collect it.

GDPR and CPRA are very similar in what data is covered and the "right to be forgotten".

We use GDPR because it includes broader definitions of personal information than US laws.

We may process your Personal Data because:

- We need to perform a contract with you
- You have given us permission to do so
- The processing is in our legitimate interests, and it is not overridden by your rights
- For payment processing purposes
- To comply with the law

Overview of WISP

- Plan establishes administrative, technical, and physical safeguards for protecting PII
- Compliance with Plan
- Record Retention
- Handling of PII
 - Storage, Access, Transmission, Disposal
- Physical Controls
- IT Policies and Procedures
 - Electronic Access, Network Security, & Encryption
- Training
- Third Party Service Providers
- Risk Assessment & Incident Management
- GDPR Appendix



Passwords, Two-Factor, and SSO

We protect data by securing our logins using multiple methods:

- **Passwords**
 - Long and complex
 - Different for each account
- **Two-Factor Authentication (MFA)**
- **Single Sign-On (SSO)**

Passw0rds

What are good practices?

- Long random passwords that contain upper, lower, number, and special characters

Great Passwords:

- FeTl(y4dGRzI=1V(dCe[
- &>axu9"wqxPkS=?yp>
- '\7%Xv9D6n]h}=v@[OH
- pqC{CmrrH"VGW:M(2:^\{

Good Passwords:

- M00nL!ghtPa\$\$ingT!me
- TR33L!ghtNa!IH0use
- El3c+r!c\$kyLimitD0g
- Fluff%#34rPoTatoS0up

Bad Passwords:

- Passw0rd!
- G4ry1960!
- D4nF3b83
- 55_W4!!\$_3

When to use:

- “Great” passwords – Whenever you can
- “Good” passwords – When remembering a good password is too difficult
(e.g. network login or KeyPass database)
- “Bad” passwords – There is no need for a bad password – EVER (as in Never Ever!)

Why? – Cyber Warfare Comes Home

Cyber criminals are trying to get into PG Calc...

(and probably your personal accounts too!)

Date	User	Application	Location		Status	Multifactor Authentication Result
12/5/2023	Nancy Cioto	Microsoft Azure PowerShell	Poienita, Mures, RO	Romania	Failure	Error validating credentials due to invalid username or password.
12/5/2023	marcomm	Microsoft Azure PowerShell	Plovdiv, Plovdiv, BG	Bulgaria	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.
12/5/2023	Louise Sainato	Microsoft Azure PowerShell	Velikiye Luki, Pskovskaya Oblast', RU	Russia	Failure	Sign-in was blocked because it came from an IP address with malicious activity
12/5/2023	Lee O'Leary	Microsoft Azure PowerShell	Ceske Budejovice, Jihocesky Kraj, CZ	Czech Republic	Failure	Error validating credentials due to invalid username or password.
12/5/2023	Julie Goldenberg Hay	Microsoft Azure PowerShell	Aberdeen, Hong Kong, HK	Hong Kong	Failure	Error validating credentials due to invalid username or password.
12/5/2023	PG Calc Sales Team	Microsoft Azure PowerShell	Varna, Varna, BG	Bulgaria	Failure	Error validating credentials due to invalid username or password.
12/5/2023	Ellen Rakatansky	Microsoft Azure PowerShell	Aberdeen, Hong Kong, HK	Hong Kong	Failure	Error validating credentials due to invalid username or password.
12/5/2023	Edie Matulka	Microsoft Azure PowerShell	Pateros, National Capital Region, PH	Philippines	Failure	Error validating credentials due to invalid username or password.
12/5/2023	David Wolfe	Microsoft Azure PowerShell	Moskva, Moskva, RU	Russia	Failure	Sign-in was blocked because it came from an IP address with malicious activity
12/5/2023	Andrea Yelle	Microsoft Azure PowerShell	Zhongzheng District, Taipei, TW	Taiwan	Failure	Error validating credentials due to invalid username or password.
12/5/2023	Andrew S. Palmer	Microsoft Azure PowerShell	Ivanovo, Ivanovskaya Oblast', RU	Russia	Failure	Error validating credentials due to invalid username or password.
12/5/2023	Admin Reports	Microsoft Azure PowerShell	Xinyi, Taipei, TW	Taiwan	Failure	Error validating credentials due to invalid username or password.
12/4/2023	Ellen Rakatansky	Office 365 Exchange Online	Islington, Greater London, GB	United Kingdom	Failure	Sign-in was blocked because it came from an IP address with malicious activity
12/4/2023	Ellen Rakatansky	Office 365 Exchange Online	Islington, Greater London, GB	United Kingdom	Failure	Sign-in was blocked because it came from an IP address with malicious activity
12/1/2023	Support	Microsoft Azure PowerShell	Aberdeen, Hong Kong, HK	Hong Kong	Failure	Error validating credentials due to invalid username or password.
12/1/2023	Nancy Cioto	Microsoft Azure PowerShell	Aberdeen, Hong Kong, HK	Hong Kong	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.
12/1/2023	marcomm	Microsoft Azure PowerShell	Xizhi, New Taipei, TW	Taiwan	Failure	Error validating credentials due to invalid username or password.
12/1/2023	Louise Sainato	Microsoft Azure PowerShell	Varna, Varna, BG	Bulgaria	Failure	Error validating credentials due to invalid username or password.
12/1/2023	Lee O'Leary	Microsoft Azure PowerShell	Ruse, Ruse, BG	Bulgaria	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.
12/1/2023	Julie Goldenberg Hay	Microsoft Azure PowerShell	Zhongxi District, Tainan, TW	Taiwan	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.
12/1/2023	PG Calc Sales Team	Microsoft Azure PowerShell	Sevlievo, Gabrovo, BG	Bulgaria	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.

Email Phishing

Sync error (Office Feature ID: 13092)



0365 Mail <infoc@4d53f23b03cb47d189b1886b0475bc37.lacit.org>

Gary Pforzheimer

Wednesday, July 18, 2018 at 2:49 PM

[Show Details](#)

At 11:32 AM, your mailbox gary@pgcalc.com failed to sync and returned (5) incoming mails.

Syncing failed to go through due to invalidation of your mailbox within the past 15 days.

[Recover Messages](#)

365 Message Center


<https://www.tjcarwash.co.nz/8/?login=gary@pgcalc.com>

NEW PAY-CHECK UPDATE!!



Warren Bailey <sareteya92634gdy@gmail.com>

To: David Kelly

 You forwarded this message on 8/3/2022 2:18 PM.

Hello Morning,

Quick One - I changed my bank recently and I want to add it up as my new direct deposit details.

Can I just send you the info directly to help me re-update it ?

Regards.

Warren Bailey

Business Continuity

Business continuity is the advance planning and preparation undertaken to ensure that an organization will have the capability to operate its critical business functions during emergency events.

Events can include natural disasters, a business crisis, pandemic, workplace violence, or any event that results in a disruption of your business operation.

It is important to remember that you should plan and prepare not only for events that will stop functions completely but for those that also have the potential to adversely impact services or functions.

(Source: mha-it.com)

Anti- Fraud

Anti-Fraud is the attempt to counter fraud.

What is fraud so we know what we're up against?

In the broadest sense, fraud can encompass any crime for gain that uses deception as its principal modus operandi. More specifically, fraud is defined by Black's Law Dictionary as:

A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.¹

Consequently, fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means.

Fraud against a company can be committed either internally by employees, managers, officers, or owners of the company, or externally by customers, vendors, and other parties. Other schemes defraud individuals, rather than organizations.

(Source: acfe.com)

Cloud Storage

Cloud storage is a place on the internet where content can be stored. It is also called file sharing. This is separate from the PG Calc network. The use of cloud storage can circumvent security control put in place to protect both internal and client information.

Examples of cloud storage are:

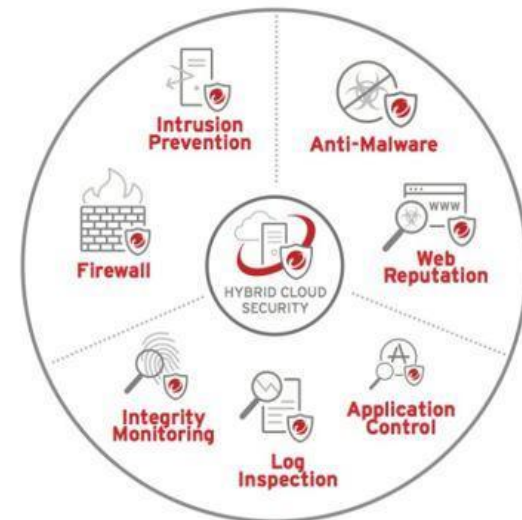
- Google Drive
- DropBox
- Box
- BackBlaze
- Wasabi
- iCloud
- Cloud Drive
- WeTransfer

Some people need cloud storage access to do their job, and they have been granted a documented, approved security exception.

End-Point Detection & Protection (EDR)

End point detection and protection (EDR) is a blanket term that refers to software that blocks computer viruses, trojans, ransomware attacks, and implements a firewall, URL protection, IDS and IPS. When there is an EDR “event”, it gets logged, and IT gets an alert. IT can use the logs for forensics research to determine if a breach or other security issue occurred.

Frequently it is called anti-virus software, but the product PG Calc uses covers more than just viruses.



Compliance

Compliance is a big and vague term that can cover a lot of subtopics. Our SOC audit looks to tackle compliance as broadly and as thoroughly as possible.

Many of our bank, hospital, and education clients are asking us to respond to compliance questionnaires.

It is time consuming but makes us better in the end by highlighting our potential weaknesses and showing us more secure ways to do things better.

It also validates the things we are doing correctly!

AI – Artificial Intelligence

- AI uses the data a user feeds it and unless you've read the terms of service **at the time of use**, you don't know what they might do with the data entered.
- The feeding of sensitive data (such as internal or client data) *might* be handing that data to AI processors that lack sufficient controls.
- We are restricting use of AI engines and will continue to do so aggressively.
- At some point, we'd like the use of unapproved AI to be an explicitly articulated offense with repercussions of up to and including termination.
- An AI Policy will be coming soon – Our goal is in the next four weeks.
- We'd like to have a vetted and controlled AI vendor

Anti-Harassment & Anti-Discrimination

- **Harassment is a bad thing and will get you fired**
 - There are laws protecting against harassment
- **There are laws protecting minorities against discrimination**
 - The new administration cannot unilaterally remove those protections or state protections
- **There will be additional qualified training coming soon**
 - Timeframe: TBD
- **In the interim, please refer to the PG Calc Handbook**
 - See Pages: 8, 42, 45, 48, 53, 61, 64, 67, 71, 74, 77, 86

What's Coming Next...?

- **NIST 800-53 v5** — This is a two-year time horizon
 - **Password Standard Changes** (Once per year!)
- **Email Phishing campaigns**
 - We now have software – Failure will require retraining
- **FIDO2** (maybe...)
 - Passwordless Authentication
- **Office365 Tenant Merge**
 - March 22nd - 25th ?
- **Phone System Migration** (TBD)
- **Machine Backups** (Druva)
- **SOC Audit** (Oct/Nov 2025)
 - Audit Period: 11/15/2024 to 11/15/2025
 - GiftWrap, PGM Anywhere, Gift Admin Services, Endowment Sub-Accounting, Marketing Services, Impactfully, FS Admin

Questions & Answers

