Welcome

Our Presentation

Will Begin at 12pm

- All viewers are muted. Audience cameras cannot be turned on.
- Who's with us today? Feel free to share your nonprofit's name in the chat box.

PRO BONO™
PARTNERSHIP / ATLANTA

Data Governance for Nonprofits: Advancing Trust, Compliance, and Impact

Misty Peterson

Counsel

Jillian Simons

Associate

August 15, 2023

Mission of
Pro Bono Partnership of Atlanta

To provide free legal assistance to community-based nonprofits that serve low-income or disadvantaged individuals.

We match eligible organizations with volunteer lawyers from the leading corporations and law firms in Atlanta who can assist nonprofits with their business law matters.

Client Criteria

In order to be a client of Pro Bono Partnership of Atlanta, an organization must:

- Be a 501(c)(3) nonprofit.
- Be located in or serve the greater Atlanta area.
- Serve low-income or disadvantaged individuals.
- Be unable to afford legal services.

Visit our website at www.pbpatl.org to apply.

PBPA Learning Center for Georgia Nonprofits

www.pbpatl.org/resources

ARTICLES

WORKSHOPS

WEBCASTS

PODCASTS

PRO BONO™
PARTNERSHIP/ATLANTA

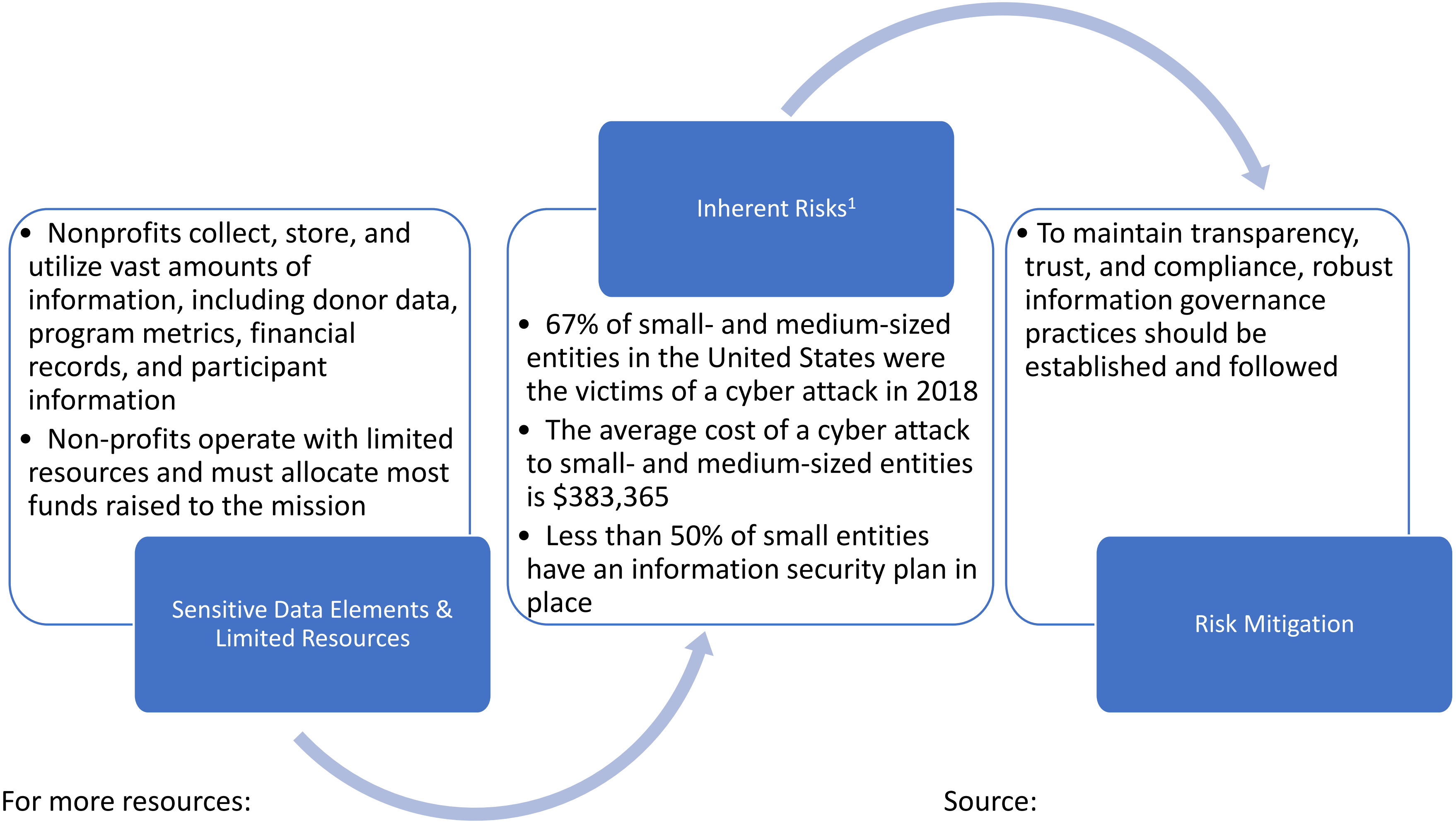
Legal Information

This webinar presents general guidelines for Georgia nonprofit organizations and should not be construed as legal advice. Always consult an attorney to address your particular situation.

Agenda

1. Overview of Data Privacy Responsibilities and Risks
2. Applicable Laws, Regulations, and Guidance – Federal and Georgia
3. Cyber Threats to Organizations
4. Risks of Using Online Marketing and Advertising Tools and AI-Enabled Apps
5. Risk Management Preventative Measures

Overview of Data Privacy Responsibilities and Risks



Sensitive Data Elements & Limited Resources

- Nonprofits collect, store, and utilize vast amounts of information, including donor data, program metrics, financial records, and participant information
- Non-profits operate with limited resources and must allocate most funds raised to the mission

Inherent Risks[1]

- 67% of small- and medium-sized entities in the United States were the victims of a cyber attack in 2018
- The average cost of a cyber attack to small- and medium-sized entities is $383,365
- Less than 50% of small entities have an information security plan in place

Risk Mitigation

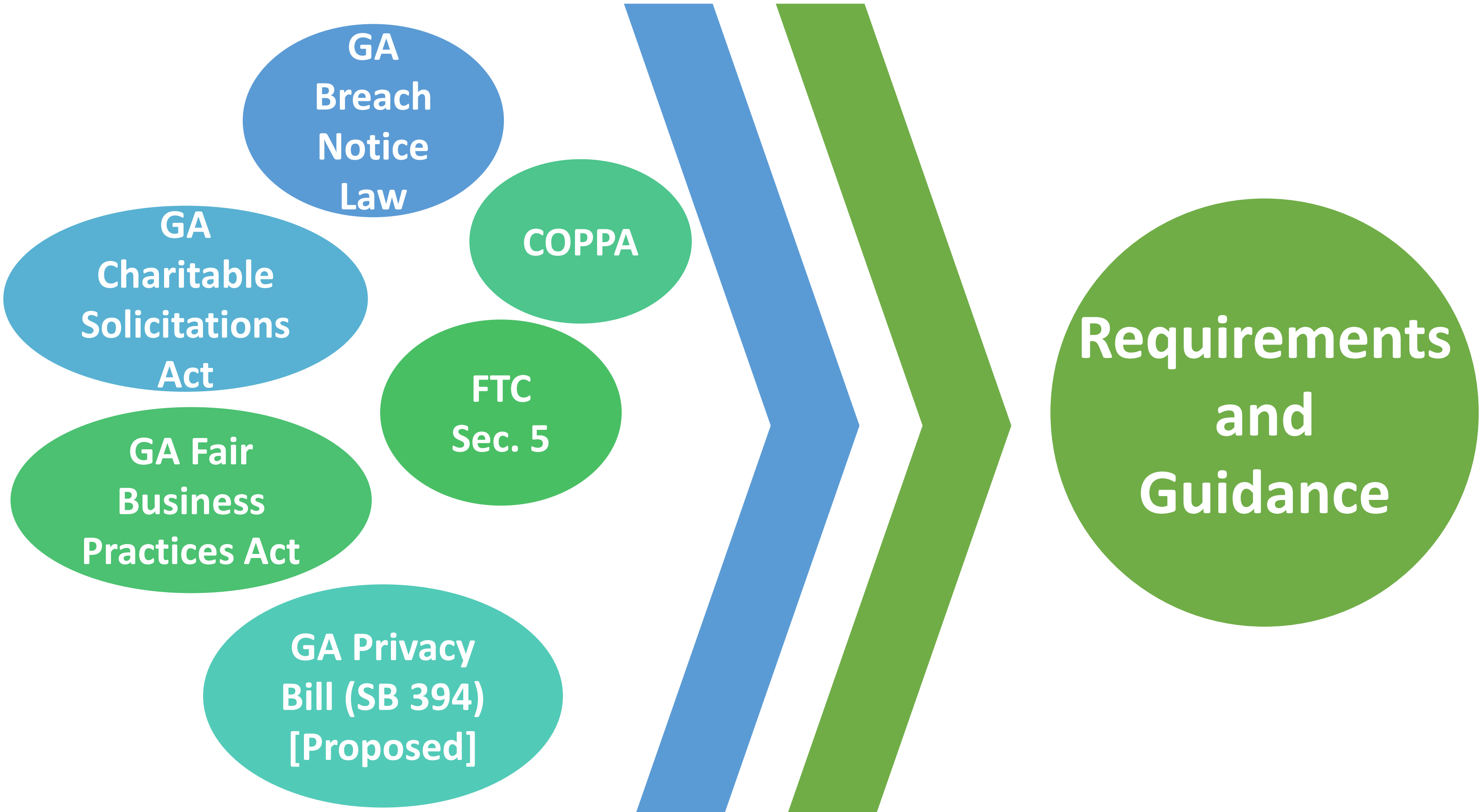
- To maintain transparency, trust, and compliance, robust information governance practices should be established and followed

For more resources:
https://pbpatl.org/learning-center
https://tnpa.org/membership/webinars-on-demand

Source:
Ponemon Institute

PRO BONO™
PARTNERSHIP / ATLANTA

Applicable Laws, Regulations, and Guidance – Federal and Georgia



GA Breach Notice Law

COPPA

GA Charitable Solicitations Act

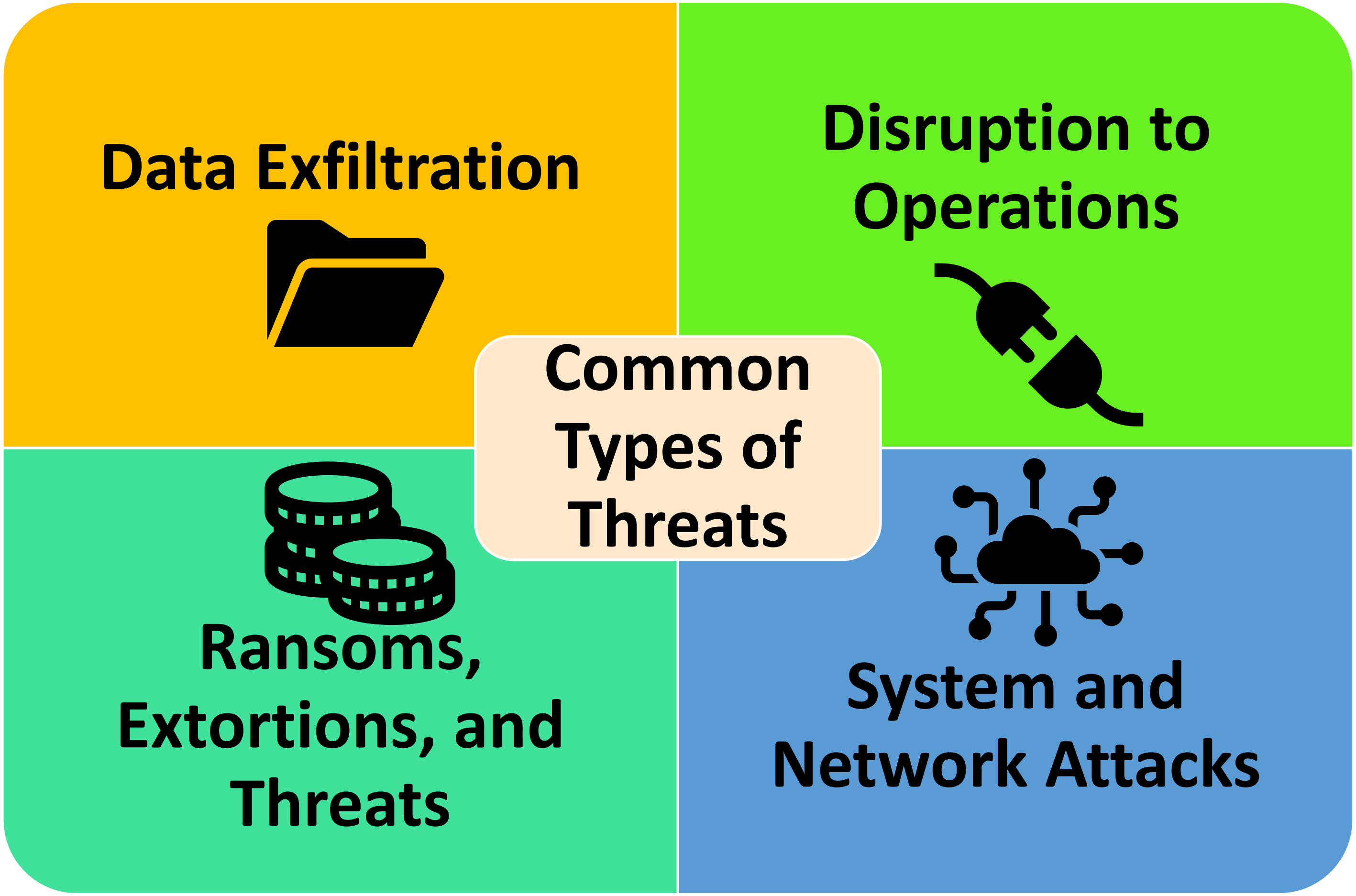
FTC Sec. 5

GA Fair Business Practices Act

GA Privacy Bill (SB 394) [Proposed]

Requirements and Guidance

Cyber Threats to Organizations



Common Types of Threats

Data Exfiltration

Disruption to Operations

Ransoms, Extortions, and Threats

System and Network Attacks

PRO BONO™
PARTNERSHIP/ATLANTA

Risks of Using Online Marketing and Advertising Tools and AI Apps

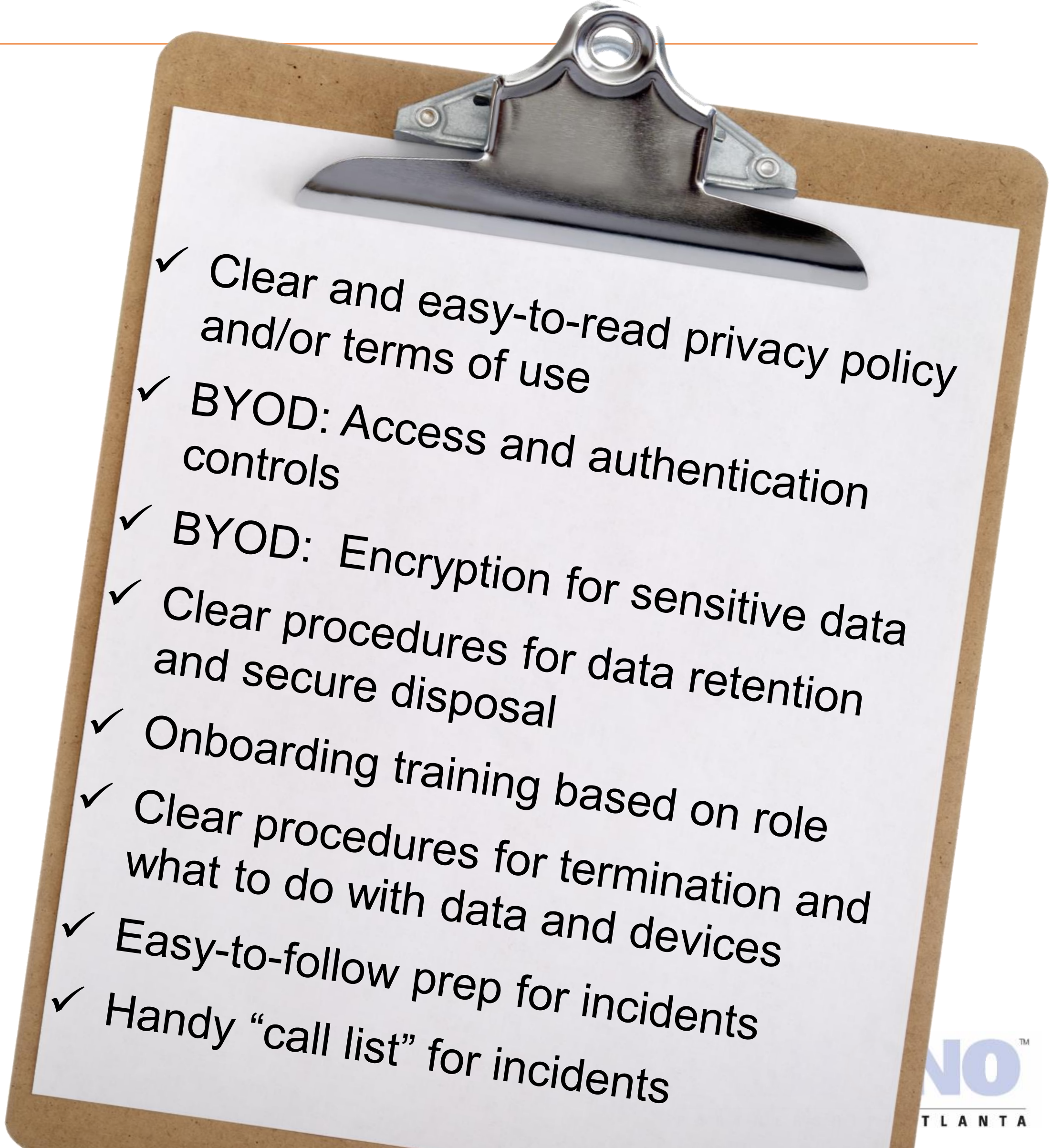
Web Beacons

Third-Party Pixels

AI-Enabled Apps

Risk Management Preventative Measures

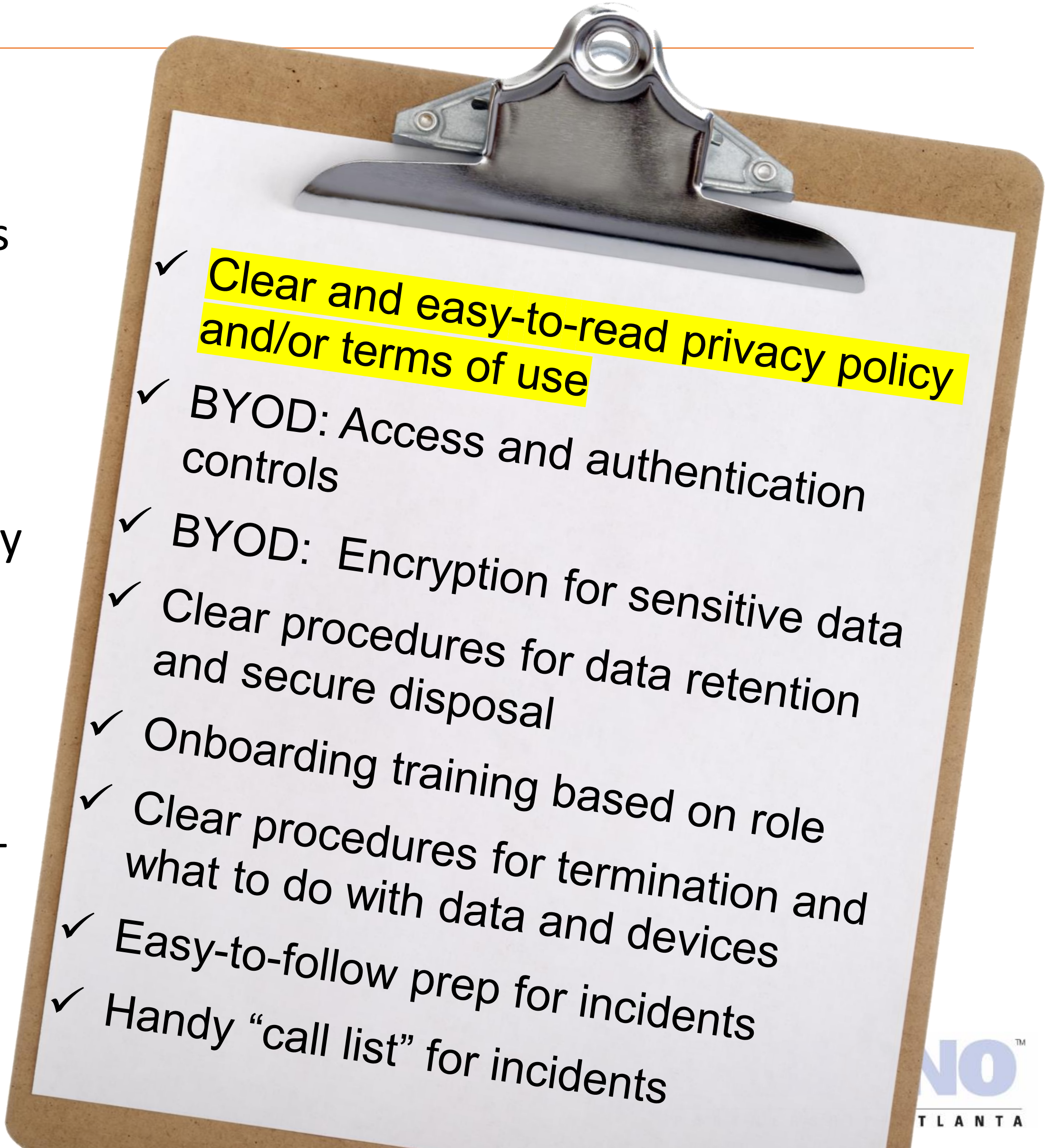
Best practices for cyber and privacy hygiene



- ✓ Clear and easy-to-read privacy policy and/or terms of use
- ✓ BYOD: Access and authentication controls
- ✓ BYOD: Encryption for sensitive data
- ✓ Clear procedures for data retention and secure disposal
- ✓ Onboarding training based on role
- ✓ Clear procedures for termination and what to do with data and devices
- ✓ Easy-to-follow prep for incidents
- ✓ Handy “call list” for incidents

Risk Management Preventative Measures

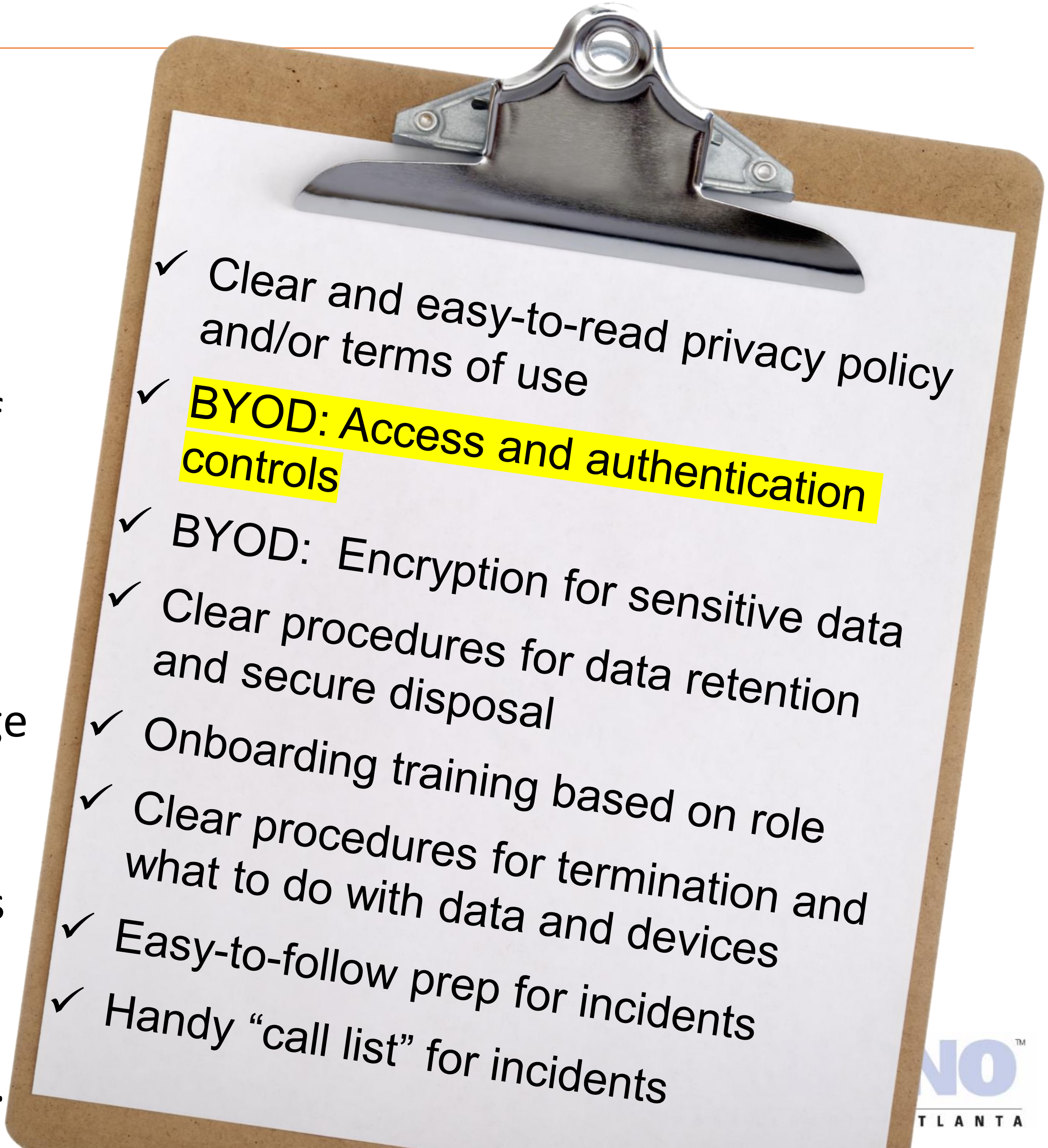
- The policy and/or terms should clearly inform visitors about the types of personal information collected and describe in detail how it is collected, processed, retained and, if relevant, why it is shared or sold to a third party.
- More resources and best practices:
  - https://pbpatl.org/best-practices-for-a-legally-compliant-website



- ✓ Clear and easy-to-read privacy policy and/or terms of use
- ✓ BYOD: Access and authentication controls
- ✓ BYOD: Encryption for sensitive data
- ✓ Clear procedures for data retention and secure disposal
- ✓ Onboarding training based on role
- ✓ Clear procedures for termination and what to do with data and devices
- ✓ Easy-to-follow prep for incidents
- ✓ Handy “call list” for incidents

Risk Management Preventative Measures

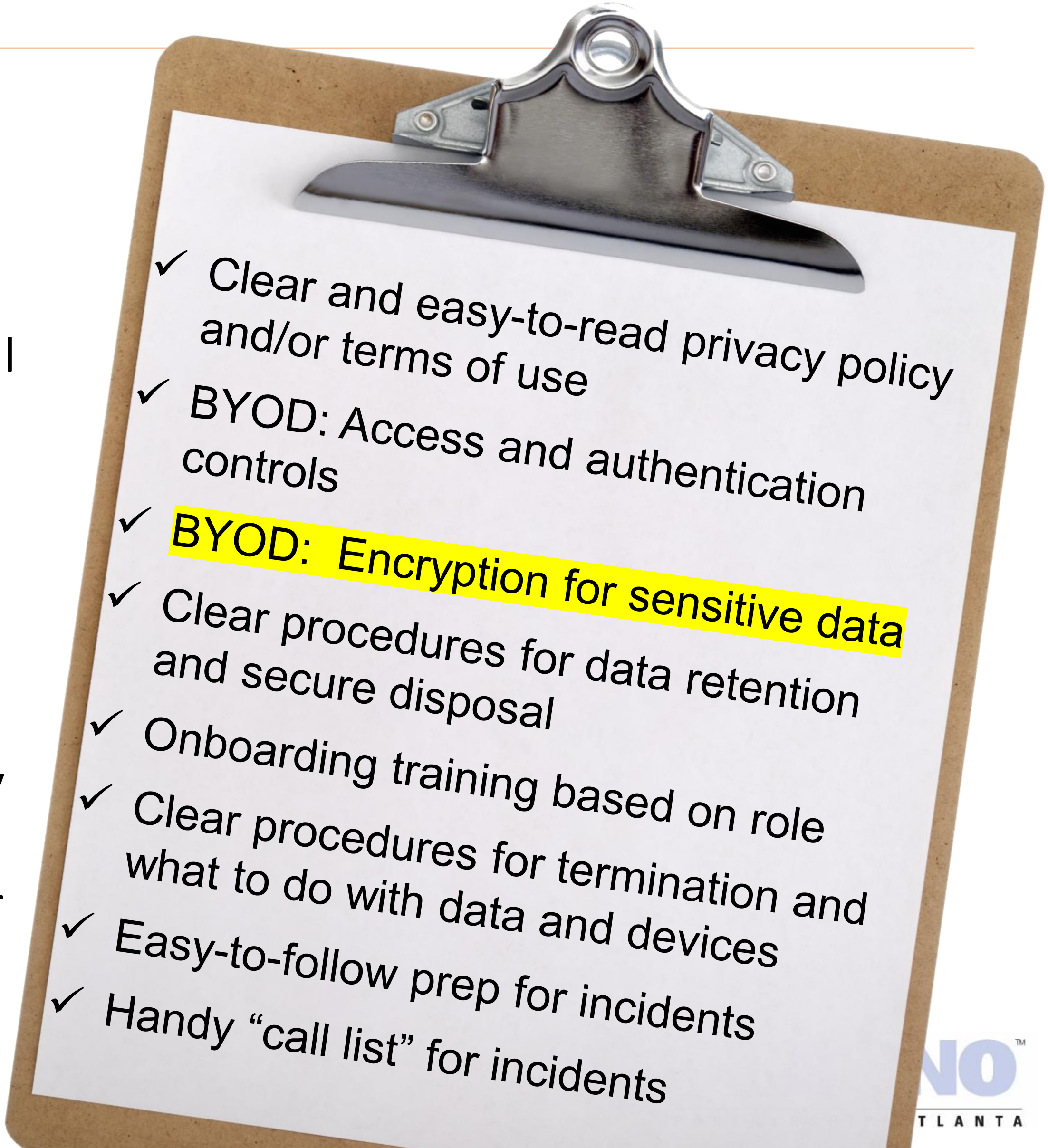
- Sensitive data should be accessible only to those employees who have a legitimate business need.
- Require strong passwords of at least 12 characters that combine upper and lowercase letters, numbers and symbols.
- Require employees to change passwords regularly.
- Limit the number of unsuccessful log-in attempts in order to limit password-guessing attacks.
- Multi-Factor Authentication.



- ✓ Clear and easy-to-read privacy policy and/or terms of use
- ✓ BYOD: Access and authentication controls
- ✓ BYOD: Encryption for sensitive data
- ✓ Clear procedures for data retention and secure disposal
- ✓ Onboarding training based on role
- ✓ Clear procedures for termination and what to do with data and devices
- ✓ Easy-to-follow prep for incidents
- ✓ Handy “call list” for incidents

Risk Management Preventative Measures

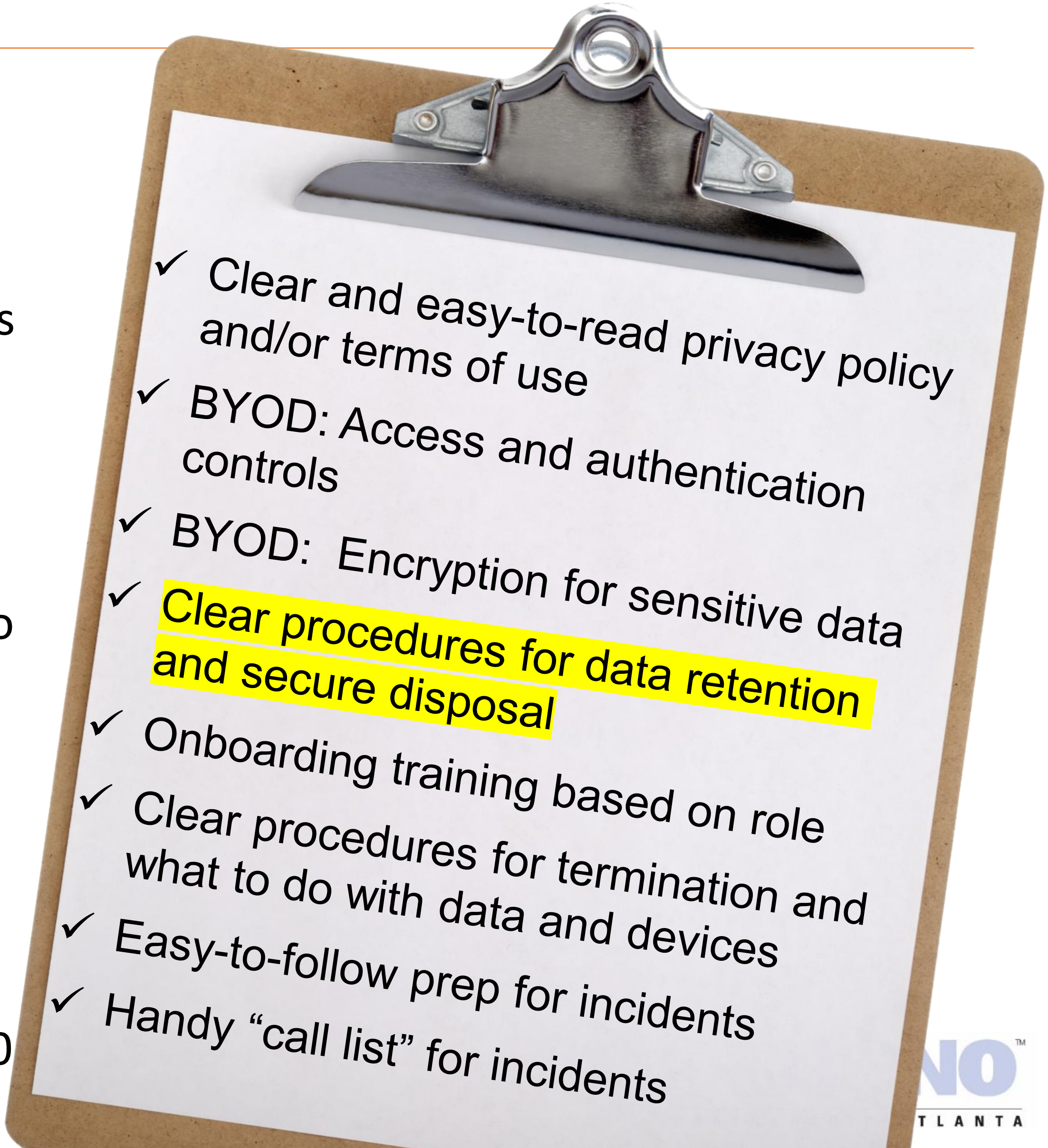
- Encrypt devices, drives, backup tapes, thumb drives and cloud storage solutions containing sensitive personal information.
- Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network.
- Use Transport Layer Security (TLS) encryption for your website to help protect your customers' privacy.



- ✓ Clear and easy-to-read privacy policy and/or terms of use
- ✓ BYOD: Access and authentication controls
- ✓ BYOD: Encryption for sensitive data
- ✓ Clear procedures for data retention and secure disposal
- ✓ Onboarding training based on role
- ✓ Clear procedures for termination and what to do with data and devices
- ✓ Easy-to-follow prep for incidents
- ✓ Handy "call list" for incidents

Risk Management Preventative Measures

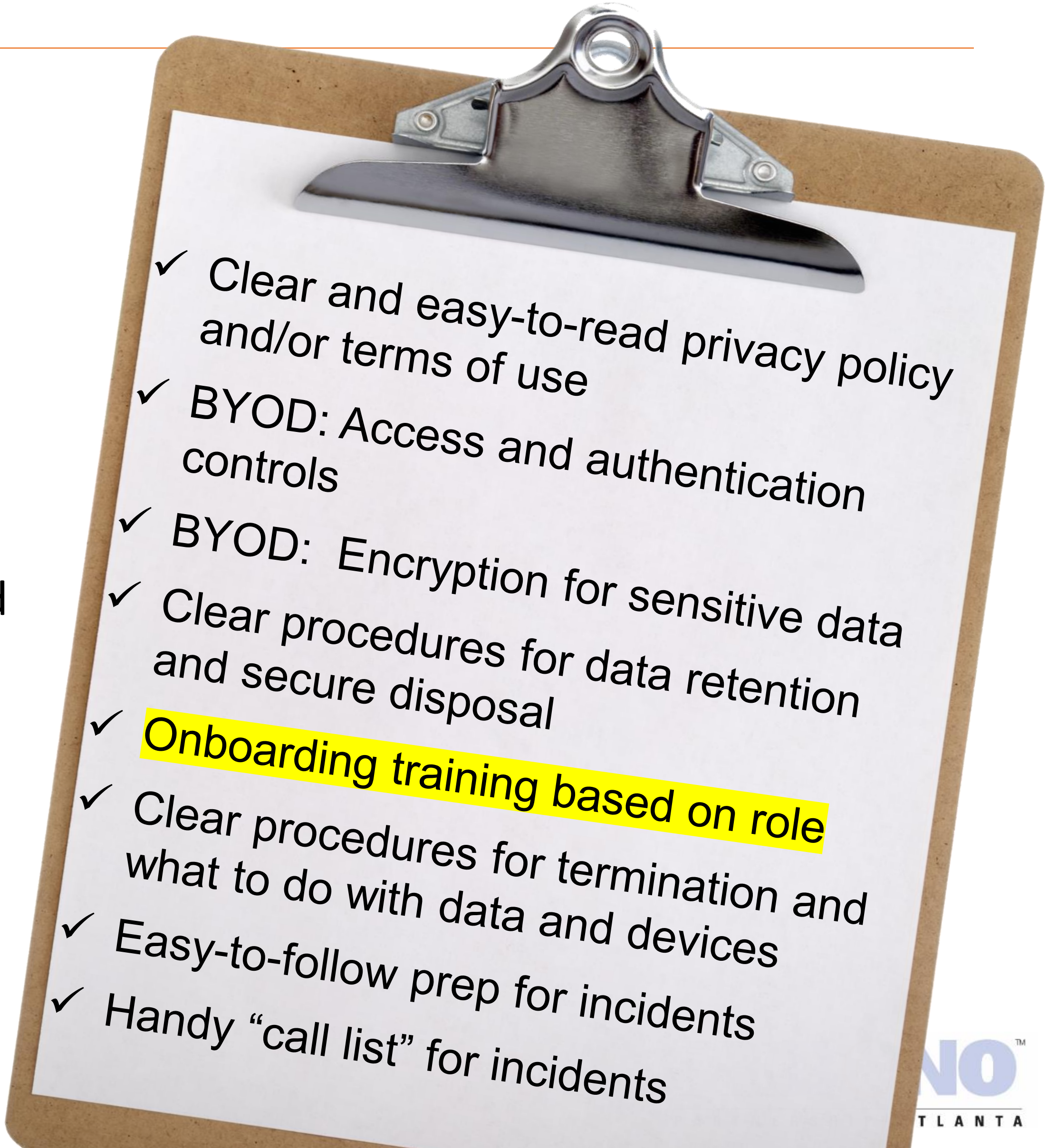
- Ensure sensitive data is destroyed properly.
- Paper documents containing sensitive data should be shredded, and computer files should be securely wiped clean from hard drives and devices.
- Delete software, apps, and social media accounts you no longer use.
- Clean out old emails and empty deleted folders.
- More resources and best practices:
  - https://pbpatl.org/wp-content/uploads/2020/06/Key_policies.pdf



- ✓ Clear and easy-to-read privacy policy and/or terms of use
- ✓ BYOD: Access and authentication controls
- ✓ BYOD: Encryption for sensitive data
- ✓ Clear procedures for data retention and secure disposal
- ✓ Onboarding training based on role
- ✓ Clear procedures for termination and what to do with data and devices
- ✓ Easy-to-follow prep for incidents
- ✓ Handy “call list” for incidents

Risk Management Preventative Measures

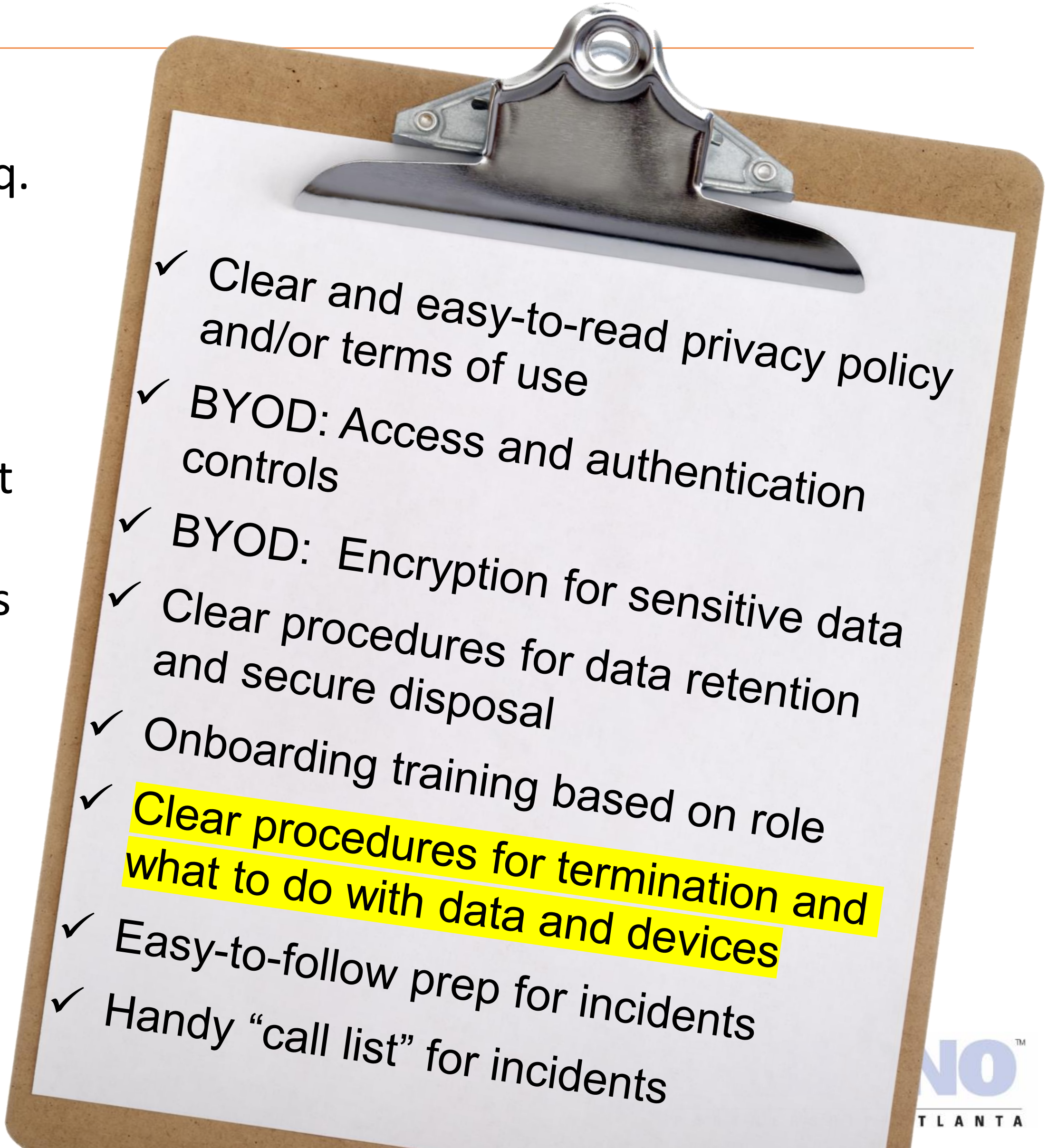
- Make sure employees are trained on how to recognize phishing and tech support scams and how to avoid downloading malware.
- Establish rules for safe Internet browsing, including using only secure, encrypted websites when entering personal or financial information.



- ✓ Clear and easy-to-read privacy policy and/or terms of use
- ✓ BYOD: Access and authentication controls
- ✓ BYOD: Encryption for sensitive data
- ✓ Clear procedures for data retention and secure disposal
- ✓ Onboarding training based on role
- ✓ Clear procedures for termination and what to do with data and devices
- ✓ Easy-to-follow prep for incidents
- ✓ Handy "call list" for incidents

Risk Management Preventative Measures

- Georgia Law § 10-15-1 et seq. requires that business records containing sensitive information be disposed of properly.
- Have policies in place so that when personnel leave your employ, their login privileges are terminated.
- More resources and best practices:
  - https://pbpatl.org/the-departure-lounge-offboarding-nonprofit-employees



✓ Clear and easy-to-read privacy policy and/or terms of use

✓ BYOD: Access and authentication controls

✓ BYOD: Encryption for sensitive data

✓ Clear procedures for data retention and secure disposal

✓ Onboarding training based on role

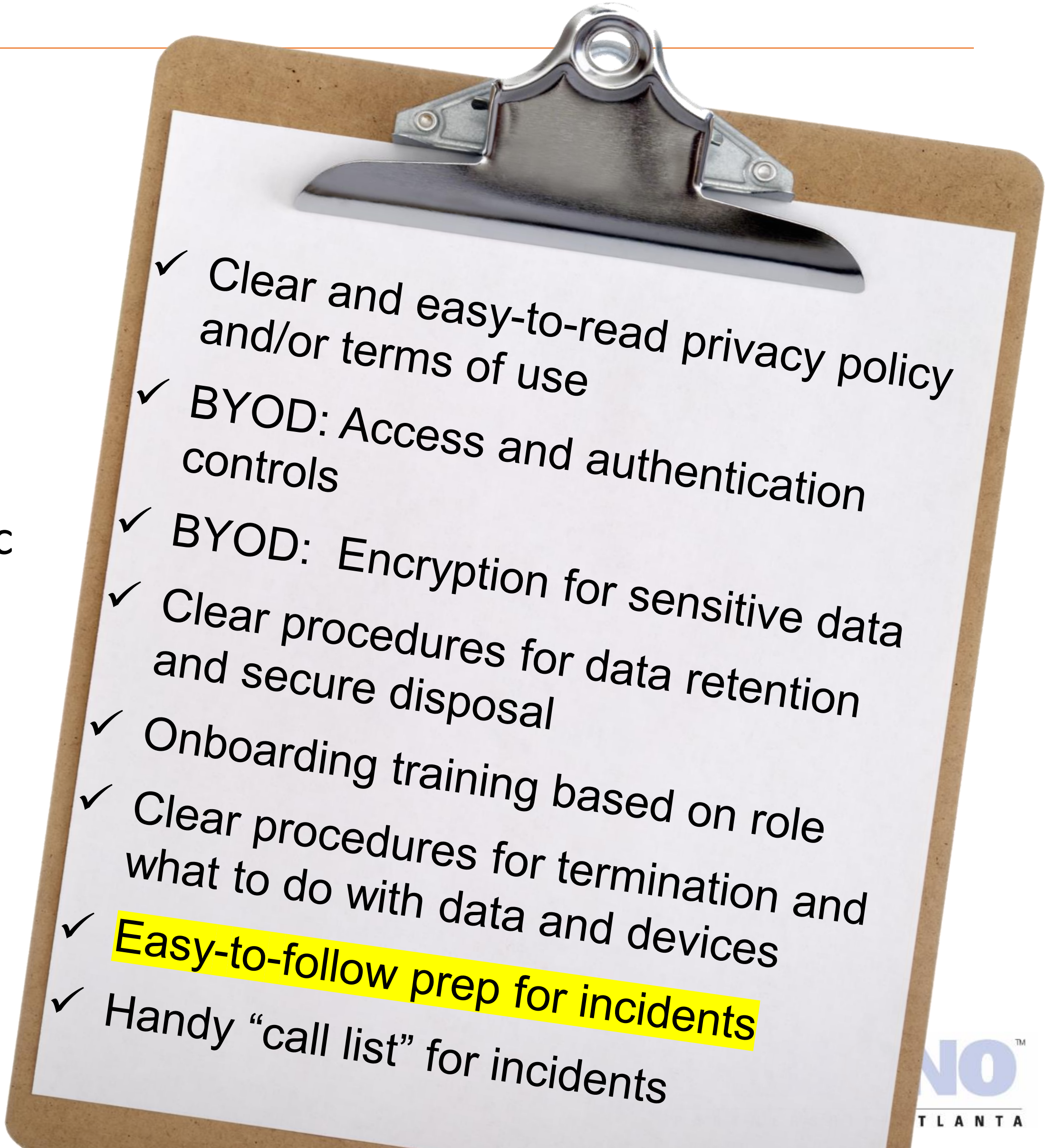
✓ Clear procedures for termination and what to do with data and devices

✓ Easy-to-follow prep for incidents

✓ Handy "call list" for incidents

Risk Management Preventative Measures

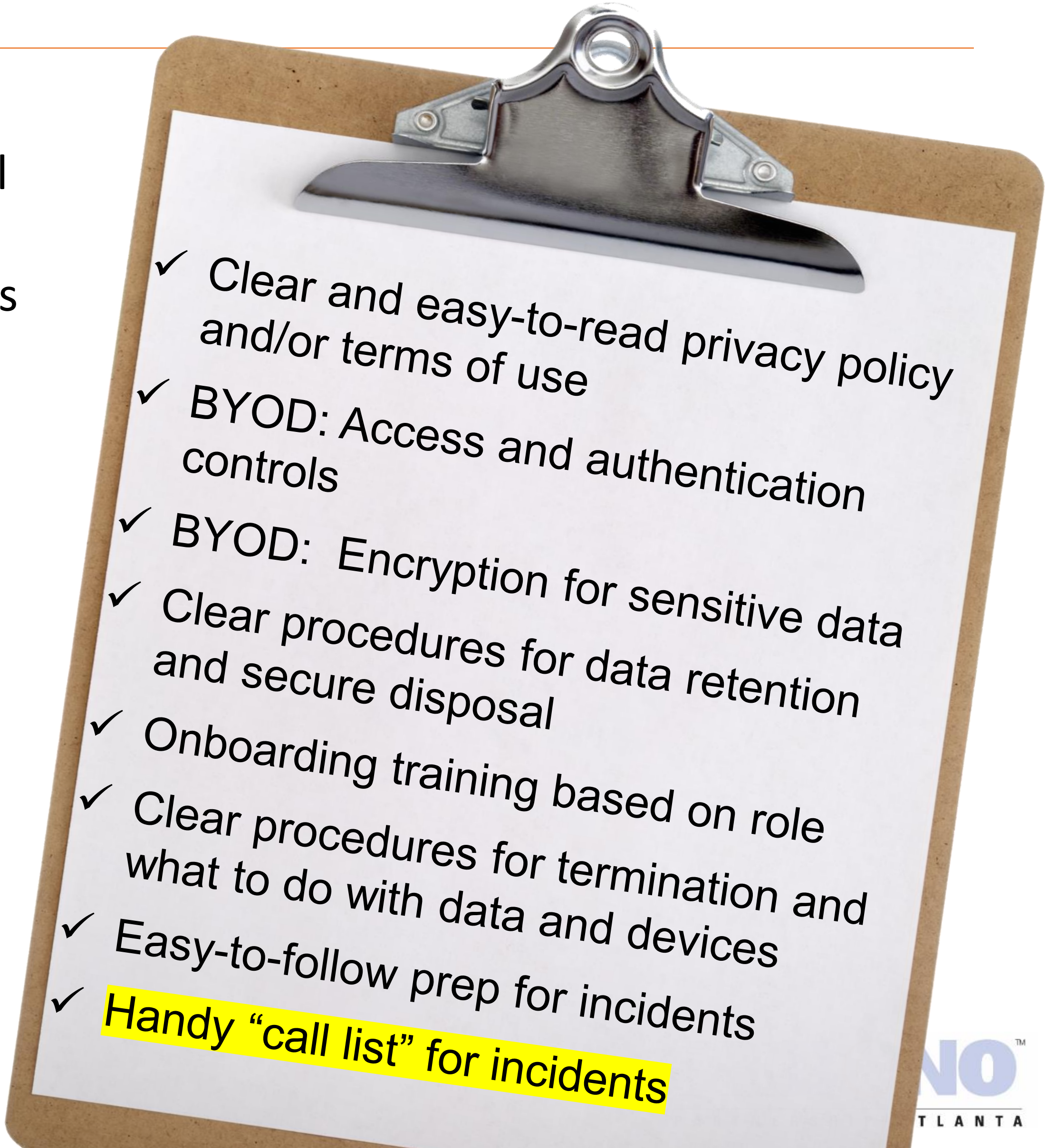
- Create an incident response checklist.
- Conduct incident response training.
- More resources and best practices:
  - https://pbpatl.org/webcast-data-breach-prevention-detection-response



- ✓ Clear and easy-to-read privacy policy and/or terms of use
- ✓ BYOD: Access and authentication controls
- ✓ BYOD: Encryption for sensitive data
- ✓ Clear procedures for data retention and secure disposal
- ✓ Onboarding training based on role
- ✓ Clear procedures for termination and what to do with data and devices
- ✓ Easy-to-follow prep for incidents
- ✓ Handy “call list” for incidents

Risk Management Preventative Measures

- Create an easy-to-access call list in the event of an incident that is also stored as a copy outside of your systems and email:
  - Legal counsel
  - IT support/third-party vendors
  - Internal and external stakeholders
  - Law enforcement (FBI, Secret Service, local police)



- ✓ Clear and easy-to-read privacy policy and/or terms of use
- ✓ BYOD: Access and authentication controls
- ✓ BYOD: Encryption for sensitive data
- ✓ Clear procedures for data retention and secure disposal
- ✓ Onboarding training based on role
- ✓ Clear procedures for termination and what to do with data and devices
- ✓ Easy-to-follow prep for incidents
- ✓ Handy "call list" for incidents

Questions?

Pro Bono Partnership of Atlanta

www.pbpatl.org

Upcoming Webcasts & Workshops Calendar

Event Listings

Nonprofit Notes Monthly Newsletter & Legal Alerts

Sign-Up

PRO BONO™

PARTNERSHIP / ATLANTA