CYBER DEFENSE FOR SMBs

DATA AUDIT WORKSHEET

A data audit is the process of determining what information your businesses possesses, where it is stored, how valuable it is, and how it is secured. Going through the process may alert you to potential information security risks you might not have thought about previously. Use this worksheet to document the steps of your data audit.

Data my company collects

- List standard Personally Identifiable Information (PII), that is, any information you collect that can be used to distinguish or trace an individual's identity. This includes name, date of birth, address, telephone number, email, social security number, ID number (such as driver's license number), IP address, credit card numbers, and login credentials.
- Also consider "Special Categories Information," such as racial or ethnic origin, health information, political opinions, religious beliefs, sexual or gender identity, and job position and workplace.

Location of Data

- Be specific with both the data storage location and geographic location: POS data is stored on a server in our Naples office; our customer list backup is on an external hard drive in the IT safe at headquarters.

Value of Data

- Rank each piece or category of data by its value to your business as either high- or low-value. PII and intellectual property are always high-value. Any data that is already widely available to the public, such as a menu or product list, is low-value.

Security Safeguards

- Review the Data Protections Best Practices section and note the cybersecurity measures that you already in place, such as restricted access, password protection, and encryption.

Who Has Access?

- Write down each person or group that has access to the data.

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

Data My Company Collects	Location of Data	Value of Data	Security Safeguards	Who Has Access?