A2J | TECH

Cybersecurity Checklist

This series of cybersecurity checklists is designed to assist you in evaluating your firm's cybersecurity requirements and current protocols, if any. By using these checklists, you will be able to assess the types of sensitive data your firm stores, how it is stored, who has access to it, and the associated risks. Between these checklists and our accompanying blogposts, you'll be able to evaluate and plan your own incident response and recovery policies to ensure your firm knows exactly what to do in case of a cybersecurity breach.

#1-STORING

PERSONALLY IDENTIFYING INFORMATION (PII)

1. Identify each item of personally identifying information (PII) and where it's stored (Example: "Client social security numbers stored in the cloud-based case management system)

Once identified, evaluate each item for the following:

- [ ] Can the objectives of the firm, such as representing clients to the fullest ability be met without this data?

- [ ] Can the objectives of the firm be met without the data being on physical documents?

- [ ] Can the objectives of the firm be met without the data being shared with internal systems and staff members?

- [ ] Is it necessary for third-parties to have access to this data to achieve business objectives?

- [ ] Based on the above answers, does the storage or transmission method for the data need to be changed?

continued ⟶

#1-STORING
PERSONALLY IDENTIFYING INFORMATION (PII)

2. Now that you've evaluated whether or not you should be storing each "piece" of PII, for every necessary piece of information, evaluate:

- [ ] Are the systems where you store, use, or transmit the PII password-protected?
  - [ ] If this password protection exists, has it been changed from the default password?
  - [ ] Is there a policy in place to set standards for the password used on the systems? For example, length and special character requirements, or a requirement mandating changing the password after a certain period of time?
- [ ] Do you install and regularly update malware or anti-virus software for these systems?
- [ ] Do you use other protections like firewalls to protect information?
- [ ] Do you have a schedule of regular backups of the critical data to protect it in case the system is inoperable?
- [ ] What is the risk to the firm if the system becomes inoperable, on a scale from low to high?
- [ ] Is there an alert system for if the system becomes inoperable, or if someone attempts to attack the system?
- [ ] When the data is transmitted internally, is it encrypted?
- [ ] When the data is backed up for archival purposes, is it encrypted?

#2–TRAINING

EMPLOYEE CYBERSECURITY PROCEDURES

1. Identify who has access to PII or firm sensitive information, and to what extent:

- [ ] Do your employees, independent contractors, vendors, or clients have access to PII or other sensitive and confidential information?

If so, make sure you evaluate the following:

- [ ] Is access to PII or other sensitive information necessary for the employee's or third-party's ability to perform their role at the firm?
- [ ] Do employees, contractors, vendors, or clients only have access to the level of PII they need to fulfill their firm-related responsibilities?
- [ ] When business is terminated with employees, contractors, vendors, or clients, is their access to the data terminated immediately?
- [ ] Based on the above answers, does the storage or transmission method for the data need to be changed?
- [ ] Are employees' and vendors' system access monitored? If so, how?
- [ ] Are account credentials (login and password) used only by the person for whom it is created? In other words, do people on your team or third-parties who have accounts on your systems ever share accounts or account credentials?

continued ⟶

#2-TRAINING

EMPLOYEE CYBERSECURITY PROCEDURES

2. Define cybersecurity needs

- [ ] Does training take into account firm-specific risks, systems, and loss incident history?
- [ ] Is training generally applied to all employees, or is it tailored to their level of access to PII?
- [ ] Do you conduct training in regular intervals (e.g., quarterly or annually)?

3. Evaluate the effectiveness of your training procedures

- [ ] Have your employees completed cybersecurity training?
- [ ] Do employees understand the explicit and specific goals of cybersecurity training from the training itself?
- [ ] Is your training interactive?
- [ ] Have your employees demonstrated an understanding of the cybersecurity policies and procedures?
- [ ] Have you conducted any simulations or drills to test your employees' ability to respond to cybersecurity threats?

#3-ACCESSING
THIRD PARTIES AND INFORMATION

1. Evaluate third-party access to confidential information:

- [ ] Is it even necessary to allow this third-party access?
- [ ] How much access do they have and what prevents them from accessing all data stored by the firm?
- [ ] Have the third-party's cybersecurity practices been assessed?
- [ ] When the data is transmitted to third-parties, is it encrypted?

2. Define third-party device access

- [ ] Is the device protected or encrypted?
- [ ] Can the device be remotely wiped of data in the case it gets lost or stolen?
- [ ] Can only authorized individuals download software to the device?
- [ ] What's the risk severity level to the overall integrity of the data storage of your organization if the device is compromised?
    - This relates to the items above in discussing the separation between what the third-party can access and all of the data stored by your organization.