Cybersecurity, Information Security, and Incident Response Policy

John Bandler's Free Starter Cybersecurity Policy Version 1.2

Revised 4/19/2023

Bandler Group LLC
Bandler Law Firm PLLC

1.0 Introduction

Information is one of our most important assets and this document sets forth how we will protect it to the best of our ability. The confidentiality, integrity, and availability of our data and systems are critical to our operation and must be safeguarded from many threats, including cybercrime and natural disaster. We must protect our information systems, including devices, data, and networks. We must also comply with applicable laws, regulations, and professional or legal norms. This policy sets forth the rules for our organization and for all individuals in our organization. This document can be referred to as our "Cybersecurity Policy" and also establishes our Cybersecurity Program. All employees must read this policy.

2.0 Overview of Information Security Objectives, Principles, Controls, Requirements, and Guidance

We will employ reasonable security measures, recognizing the three objectives of information security: the protection of *confidentiality*, *integrity*, and *availability* of information assets. Information assets include our computing devices, data, online accounts, and networks. We will secure our systems by implementing reasonable safeguards (also known as "controls"). These safeguards will be *physical*, *administrative*, and *technical*. More information on these important cybersecurity principles is here.[1]

We will structure our controls according to "Bandler's Four Pillars of Cybersecurity", as detailed later in this document. We will incorporate a prioritized, risk-based approach to protect our information assets. In performing all our cybersecurity activities, we will prevent, detect, respond to, and recover from, attacks or system failures. Read more on the Four Pillars here.

We will follow applicable *external rules* relating to cybersecurity, whether legal, regulatory, contract, or matters of professional responsibility. These external rules guide our level of cybersecurity and how we investigate and respond to a potential incident. We will be reasonable and diligent, not negligent or deficient. Read more about external rules here.

We will seek and follow appropriate *external guidance and resources*. This guidance includes the "Four Pillars of Cybersecurity" and other guidance from John Bandler and other qualified sources. As our organization grows and matures, we can explore more complex frameworks and guidance, including guidance from the National Institute of Standards and Technology ("NIST").

When warranted, we will seek professional, expert guidance.

[1] All embedded links in this document point to pages at JohnBandler.com. The Appendix lists the full URLs for each article.

3.0 Implementing the Cybersecurity Policy and Program

We will apply sound governance and management over our information assets, prioritizing cybersecurity. This requires continual evaluation of risks, areas for improvement, allocation of resources, and making security a part of our organization's culture.

This document establishes our policy and program; it is our highest-level cybersecurity document. As we grow and our cybersecurity program matures, this document should be reviewed, updated, and expanded as needed. We will consider management best practices and we may decide that additional governance documentation should be developed. We can consider the Five Components for Policy Work.

We will designate a member of our organization as the "Information Security Coordinator". The Information Security Coordinator will be responsible for managing and implementing our cybersecurity program and keeping this document current. If needed, we can create an Information Governance Committee to guide our leadership on how to use and protect information assets. We will also designate an "Incident Response Team", which will include our Information Security Coordinator.

We will evaluate and manage cybercrime and information security risks appropriately and maintain an information security posture that is suitable for our risks, size, complexity, and operations.

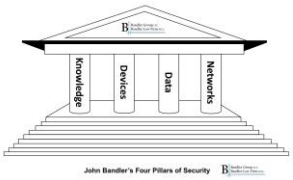
Risk management involves evaluating threats, probabilities, potential harms, and potential risk mitigation measures. We will – generally and conceptually – set our "security dial" and decide upon the appropriate level of security. Generalized risks include:

- **Cybercrime** of all types, particularly:
  - The Three Priority Cybercrime Threats
    - Data breaches
    - Ransomware
    - Email Based Funds Transfer Frauds including business email compromise (BEC) and CEO Fraud.
- **Disaster**: Fire, flood, hurricane, or other natural or person-made disaster that might damage information assets.
- The risk that someone claims we have not met our duty relating to cybersecurity.

4.0 Cybersecurity Controls (Safeguards)

We will implement reasonable cybersecurity controls (safeguards) to protect data and systems with a continual and cyclical process of review and improvement. Our cybersecurity controls will be organized using Bandler's Four Pillars of Cybersecurity. The Four Pillars is a practical, conceptual framework that focuses on:

1. *Knowledge and awareness* of cybercrime, information security threats, and technology
2. Protection of computing *devices*
3. Protection of *data*
4. Protection of *networks* and safe use of the Internet.



Our controls will be prioritized to protect against data breach, ransomware, and email-based funds transfer frauds. We will seek expert assistance where warranted.

4.1 Knowledge and awareness

Knowledge and awareness are required by *every person* in our organization. This will help us recognize and guard against cybercrime and cybersecurity threats. Knowledge improves our decision making at all levels. There will be periodic training, which can include self-directed, informal, and formal.

All employees should have sufficient knowledge and awareness about matters such as:

- Organizational cybersecurity policy (this document)
- Cybercrime threats, including
    - Social engineering (con artistry) and similar threats aimed at people
    - Email based funds transfer frauds ("business email compromise" and "CEO Fraud")
    - Phishing
    - Malware, including ransomware
    - Data breaches and data theft
    - Identity theft
- Privacy threats
- Basic information security principles
- How computers work
- How networks and the internet work
- How to implement basic security measures and make good security decisions
- The importance of cybersecurity in the home, and how security at work and home are interrelated
- How working remotely creates security risks.

4.1.1 Email-based funds transfer frauds

To help protect against email-based funds transfer frauds, we will:

- Secure our own email accounts with strong unique passwords and multi-factor authentication
- Be aware that the email accounts of others can be compromised ("hacked")
- Follow steps to reduce the risks of funds transfer frauds including:
    - Verify all funds transfer instructions with a phone call (this helps ensure the instructions are genuine)
    - Verify any changes to funds transfer instructions with a phone call
    - Request that anyone relaying funds transfer instructions conduct a similar verbal verification
    - Warn those with whom we send or receive funds about this fraud, and instruct them to verify any funds transfer instructions with us verbally.

Read more about email-based frauds here.

4.2 Device security

We will secure computing devices as the second pillar of security. These devices include desktop computers, laptops, tablets, smart phones, servers, and more. They also include networking devices like routers, switches, printers, and related hardware.

We will, organizationally and individually (where applicable):

1. Inventory all devices, and develop a process for bringing them into service (commissioning) and taking them out of service when no longer needed (decommissioning).
    a. New devices will be configured (commissioned) securely (to include change of default passwords).
    b. Old devices being removed from service will be decommissioned securely (including secure deletion of data, and removal of access to cloud accounts).
2. Ensure physical security and control over these devices. Devices will be protected from loss, damage, or theft.
3. Devices will be configured with a complex and unique password, and will auto-lock after a period of inactivity. Biometric authentication (e.g. fingerprint, facial identification) can also be configured.
    - Default passwords will be changed.
4. Device operating system and applications will be updated (patched) regularly.
5. Devices will run only necessary and reliable software.
6. Device settings will be configured securely.
7. Devices will be kept malware free, running anti-malware software and regularly scanned.
8. Devices will employ firewalls to prevent intrusion.
9. Access to devices will be controlled. User accounts will be unique and will not be shared. Passwords will not be shared.
10. Security and privacy settings will be reviewed periodically.

4.3 Data security

We will secure our data as our third pillar of security. This includes keeping certain data confidential from unauthorized access, and keeping certain data available for organizational use. Threats to our data include data breach, ransomware, natural disaster, or technical failure, so we must protect against those while being able to respond effectively as needed.

Data (and other forms of information) will be inventoried to a reasonable degree, including data stored on devices, in the cloud, and other locations. We will consider the sensitivity of data, and any duties to safeguard it or report a data breach involving it. For all data types and locations, we will consider the level of sensitivity, and:

- What consequences might result if this data were *breached* (stolen):
    - How might this breach be exploited by the attacker or other criminals?
    - What breach reporting requirements might be triggered?
- What consequences might result if our organization *lost access* to this data?
    - How would our operations be affected?
- What consequences if our data was improperly changed without authorization?

"Data" is a broad category so our review needs to consider the different *types* of data and different *places* data might be stored:

Securing data includes taking these steps

1. Secure our devices as set forth previously.
2. Inventory data (to a reasonable degree of detail).
3. Secure cloud accounts properly.
    a. Important cloud accounts must be secured by complex, unique passwords, and a second factor of authentication (multi-factor authentication, MFA, or 2FA).
    b. Important cloud accounts include email, document storage, financial, social media.
4. Access to data will be controlled.
5. User accounts will be reviewed periodically. Off-boarding for former employees will include removal of access.
6. Data will be secured in a manner commensurate with its sensitivity.
7. Some (or most) data may need to be encrypted, depending upon sensitivity.
8. Data that is no longer needed should be securely deleted.
9. Data will be backed up regularly (see next subsection).

4.3.1 Backup of data

Regular backup of data in a secure manner is essential to guard against a host of threats that could compromise data systems and the organization, as set forth previously.

10. Data will be backed up periodically and in accordance with balancing costs and risks.
11. Backups will be stored securely to protect from compromise (breach or destruction). This may include encryption.
12. Backup data will be capable of being restored within an acceptable period of time (in case the original data becomes damaged or unavailable).

4.4 Network and Internet Security

We will secure our networks and our usage of the internet as our fourth pillar of cybersecurity.

1. Network hardware will be inventoried and physically secured.
2. Routers and switches will have unique (and non-default) passwords.
3. Routers and switches will be kept updated (patched). Unneeded features will be disabled.
4. Wi-Fi networks will be encrypted and require a strong password to join. The password will be changed periodically.
5. We will evaluate network intrusion prevention and monitoring.
6. We will be conscious of the route that data takes.
7. We will try to avoid the use of, or otherwise minimize, the use of public networks.
8. Encryption of data in transit will be used whenever practical.
9. Certain data can be encrypted at the file level for transmittal.

5.0 Incident Investigation and Incident Response

We will plan and prepare for a cybercrime or cybersecurity incident, and be able to respond and investigate appropriately if such an incident or cybercrime occurs. Good planning and preparation will keep us ready and help to prevent an incident. Incident prevention remains our goal (though not every incident is preventable).

Where feasible, we will have mechanisms to monitor for and detect events and incidents so that we can learn of a potential cybercrime or other threat to our information or financial assets. We will investigate and respond to real and suspected incidents appropriately.

Appropriate legal, regulatory, and professional rules will be considered, especially data breach notification laws. During or after an incident, when legally required or otherwise appropriate, we will notify affected parties if their personal information was breached as well as appropriate government authorities. In general, reporting and notifications may need to be made to:

- Affected individuals
- State Attorneys General
- Law enforcement
- Other agencies (as appropriate or required).

Incident response will be conducted in accord with best practices and in compliance with applicable laws and regulations. We will designate members of our Incident Response Team, which will include personnel from inside the organization, supplemented with outside personnel if needed. Likewise, we will seek appropriate external expert assistance for investigation and incident response as needed. We will maintain a listing of contact information relevant for incident response and reporting.

In planning and executing the complex process of incident response, the following guidance can be considered.

- Cybersecurity for the Home and Office, by John Bandler, Chapters 14 and 15

- Cybercrime Investigations, by John Bandler and Antonia Merzon
- NIST Cybersecurity Framework
- NIST guidance for small businesses
- NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide

6.0 Conclusion

This policy document is designed to be general, concise, and reader-friendly. It exists to protect our organization and those who interact with us, including customers, clients, and employees. This also helps us comply with external laws and regulations. This document does not attempt to detail all external requirements and guidance, or anticipate every potential circumstance. As needed, consult the resources cited here, consult with our Information Security Coordinator, and seek external expert advice. This document will be reviewed annually and as changes in circumstances require, and updated as needed.

7.0 Appendix (references and resources)

Below is a list of references and resources, including those cited within the document.
Links are subject to change and articles and references might become outdated.
Seek expert assistance where warranted.

Laws and regulations:

- Consult applicable federal, state, and local laws, regulations, and seek legal advice where warranted.
- Law, https://johnbandler.com/law/
- Cyberlaw, https://johnbandler.com/cyberlaw/
- Cybersecurity Laws and Regulations 1 (general overview) https://johnbandler.com/cybersecurity-laws-and-regulations-1/
- Cybersecurity Laws and Regulations 2 (listing and brief summary of some laws and regulations), https://johnbandler.com/cybersecurity-laws-and-regulations-2/
- The NYS SHIELD Act Cybersecurity and Data Breach Law, https://johnbandler.com/new-york-cybersecurity-requirements-and-the-shield-act/

Cybercrime threats

- The Three Priority Cybercrime Threats, https://johnbandler.com/priority-cybercrime-threats/
    - Email Based Funds Transfer Frauds, https://johnbandler.com/email-based-funds-transfer-frauds/
    - Ransomware, https://johnbandler.com/ransomware/
    - Data breaches, https://johnbandler.com/data-breach/

Cybersecurity and information management basics

- Introduction to Cybersecurity and Information Security, https://johnbandler.com/introduction-cybersecurity-information-security/
- Cybersecurity Tips from John Bandler, https://johnbandler.com/cybersecurity-tips-from-john-bandler
- Bandler's Four Pillars of Cybersecurity, https://johnbandler.com/bandlers-four-pillars-of-cybersecurity/
- Five Components for Policy Work, https://johnbandler.com/five-components-for-policy-work/
    - Bandler's Three Platforms to Connect, https://johnbandler.com/bandlers-three-platforms-to-connect/
    - Policies and Procedures, https://johnbandler.com/policies-and-procedures/
    - Policies, Procedures, and Governance of an Organization, https://johnbandler.com/policies-procedures-and-governance-of-an-organization/
- Cybersecurity, Privacy, You, and Your Organization, https://johnbandler.com/cybersecurity-privacy-you-and-your-organization/
- Cybersecurity Frameworks and Guidance, https://johnbandler.com/cybersecurity-frameworks-and-guidance/

- Cybersecurity forms for the home or small office, https://johnbandler.com/cybersecurity-asset-inventory-forms-for-the-home
- Cybersecurity and Working from Home, https://johnbandler.com/cybersecurity-and-working-from-home/

Key term definitions

- Cybersecurity dial, https://johnbandler.com/cybersecurity-dial/
- Passwords, https://johnbandler.com/passwords/
- Two factor authentication (2FA, Multi factor authentication, MFA, two-step authentication), https://johnbandler.com/two-factor-authentication/
- Risk and risk management, https://johnbandler.com/risk/
- Email security, https://johnbandler.com/email-security/

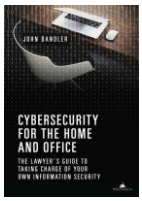
About this document

- Current version of this free cybersecurity policy, https://johnbandler.com/cybersecurity-policy-free-version/
- Current version of terms of use of this free cybersecurity policy, https://johnbandler.com/terms-of-use-free-cybersecurity-policy/

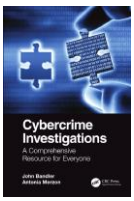
National Institute of Standards and Technology (NIST) resources

- NIST Small Business Cybersecurity Corner, https://www.nist.gov/itl/smallbusinesscyber
- NIST small business incident response guidance, https://www.nist.gov/itl/smallbusinesscyber/responding-cyber-incident
- NIST Cybersecurity Framework, https://www.nist.gov/cyberframework
- NIST Special Pub 800-61 Revision 2 Computer Security Incident Handling Guide, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Books



- *Cybersecurity for the Home and Office* (American Bar Association, 2017) by John Bandler. Book overview webpage, https://johnbandler.com/cybersecurity-for-the-home-and-office/
- *Cybercrime Investigations* (CRC Press, 2020) by John Bandler and Antonia Merzon. Book overview webpage, https://johnbandler.com/cybercrime-investigations/



8.0 Terms of Use, Disclaimer, and Ownership of Intellectual Property

These Terms of Use apply to John Bandler's complimentary ("free" or "starter") cybersecurity policy. These Terms must be left in place without modification. You may edit and adjust the rest of this document, but please leave this notice in place and as-is. I have attempted to write this in plain English and keep it short, simple, and clear.

If you do not agree to any of these terms, do not download or use this document, and delete any copies you have downloaded, printed, or otherwise made.

This document is provided without charge by John Bandler, Bandler Law Firm PLLC, and Bandler Group LLC) (collectively, "we" or "us"). We provide it to help small organizations protect themselves from the scourge of cybercrime, realizing many lack the resources and ability to hire professionals. This document is intended for small organizations that cannot afford cybersecurity advice or services. It is not tailored to any particular organization, nor is it legal or consulting advice, and no client relationship exists between you and us. This document is not a substitute for professional, expert services and assistance. A paid expert can create or update a policy, tailor it to your organization, as well as providing many other helpful services.

You use this document at your own risk. We assume no liability whatsoever and provide no warranty of any kind. You agree to hold us harmless for any bad things that might happen, and you waive all claims against us. You also agree to indemnify us for third-party claims.

We retain all intellectual property ownership rights in and to the material presented in this document, including copyright. We grant you a limited license to use this for your organization's internal use, but not to resell it, nor share it outside of your organization (unless legally required). Attribution to us of original authorship must be retained as well as noting if changes were made by you. Publishers of John Bandler's books and articles retain their rights as well.

You understand that a cybersecurity policy has value *if* it is followed, and cybersecurity requires continual improvement. An ignored policy is of little use, will not protect you from cybercrime (cybercriminals never stop), nor put you in compliance with cybersecurity laws and regulations.

For deeper understanding of this document, cybersecurity, cybercrime threats, and more, read the free articles on my website and my books. If there are terms or concepts in this document that you do not understand, look to my writings, conduct appropriate research, and seek professional and expert advice.

This document is a work-in-progress and is not perfect for everyone (no document is). We welcome any suggestions to improve it and the other resources. If you find my resources helpful, please spread the word, express appreciation, purchase my books, or consider me when your organization becomes ready to commit resources to improve cybersecurity.

The policy and these terms of use are available on my website, and may be updated occasionally.
https://johnbandler.com/terms-of-use-free-cybersecurity-policy/
https://johnbandler.com/cybersecurity-policy-free-version/