Data Security Lessons from the Federal Trade Commission (FTC)

1. **Start with Security.** Factor security into the decision-making in every department of your business – personnel, sales, accounting, information technology, etc. Make conscious choices about the kind of information you collect, how long you keep it, and who can access it, to reduce the risk of a data compromise down the road.
   a. Don't collect personal information you do not need.
   b. Hold on to information only as long as you have a legitimate business need.
   c. Don't use personal information when it's not necessary. (eg. during training sessions)

2. **Control access to data sensibly.** As soon as you've decided you have a legitimate business need to hold on to sensitive data, take reasonable steps to keep it secure. Not everyone on your staff needs unrestricted access to your network and the information stored on it. Put controls in place to make sure employees have access only on a "need to know" basis.
   a. Restrict access to sensitive data.
   b. Limit administrative access, which allows a user to make system-wide changes to your system.

3. **Require secure passwords and authentication.**

Revised 06/07/21 BL

THIS CONTENT IS PROVIDED FOR GENERAL INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE ANY ADVICE WHATSOEVER, INCLUDING BUT NOT LIMITED TO LEGAL ADVICE OR TAX ADVICE. THE INFORMATION MIGHT NOT BE UP-TO-DATE, COMPLETE, OR ACCURATE, SO PLEASE UNDERTAKE DUE DILIGENCE, INCLUDING TALKING WITH A QUALIFIED LAWYER, CPA, OR OTHER PROFESSIONAL.

   a. Insist on complex and unique passwords
   b. Store passwords securely.
   c. Guard against brute force attacks that work by typing endless combinations of characters until hackers luck into someone's password. For example, restrict the number of tries allowed for passwords.
   d. Protect against authentication bypass. Test for common vulnerabilities.

4. **Store sensitive personal information securely and protect it during transmission.** Use strong cryptography to secure confidential material during storage and transmission of sensitive data.
   a. Keep sensitive information secure throughout its lifecycle. Data doesn't stay in one place. That's why it's important to consider security at all stages.
   b. Use industry-tested and accepted methods.
   c. Ensure proper configuration. (eg. SSL certificate validation)

5. **Segment your network and monitor who's trying to get in and out.** Consider using tools like firewalls to segment your network, thereby limiting access between computers on your network and between your computers and the internet.
   a. Another useful safeguard: intrusion detection and prevention tools to monitor your network for malicious activity.
   b. Segment your network – not every computer in your system needs to be able to communicate with every other one. You can help protect

THIS CONTENT IS PROVIDED FOR GENERAL INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE ANY ADVICE WHATSOEVER, INCLUDING BUT NOT LIMITED TO LEGAL ADVICE OR TAX ADVICE. THE INFORMATION MIGHT NOT BE UP-TO-DATE, COMPLETE, OR ACCURATE, SO PLEASE UNDERTAKE DUE DILIGENCE, INCLUDING TALKING WITH A QUALIFIED LAWYER, CPA, OR OTHER PROFESSIONAL.

particularly sensitive data by housing it in a separate secure place on your network.

c. Monitor activity on your network.

6. **Secure remote access to your network.** While a mobile workforce can increase productivity, it also can pose new security challenges.

   a. Ensure endpoint security. Like a chain is only as strong as its weakest link, your network security is only as strong as the weakest security on a computer with remote access to it.

   b. Put sensible access limits in place. Not everyone who might occasionally need to get on your network should have an all-access, backstage pass.

7. **Apply sound security practices when developing new products.**

   a. Early in the development process, think through how customers will likely use the product. If they'll be storing or sending sensitive information, is your product up to the task of handling that data securely?

   b. Train your engineers in secure coding practices.

   c. Follow platform guidelines for security. There may not be a need to reinvent the wheel. Sometimes the wisest course is to listen to the experts.

   d. Verify that privacy and security features work.

   e. Test for common vulnerabilities.

Revised 06/07/21 BL

THIS CONTENT IS PROVIDED FOR GENERAL INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE ANY ADVICE WHATSOEVER, INCLUDING BUT NOT LIMITED TO LEGAL ADVICE OR TAX ADVICE. THE INFORMATION MIGHT NOT BE UP-TO-DATE, COMPLETE, OR ACCURATE, SO PLEASE UNDERTAKE DUE DILIGENCE, INCLUDING TALKING WITH A QUALIFIED LAWYER, CPA, OR OTHER PROFESSIONAL.

ISBDC@LCSC.edu 208-792-2465 IdahoSBDC.org

8. **Make sure your service providers implement reasonable security measures.**

    a. Before hiring someone, be candid about your security expectations. Take reasonable steps to select providers able to implement appropriate security measures and monitor that they're meeting your requirements.

    b. Put it in writing.

    c. Verify compliance.

9. **Put procedures in place to keep your security current and address vulnerabilities that may arise.**

    a. Securing your software and networks isn't a one and done deal. It's an ongoing process that requires you to keep your guard up.

    b. Apply software updates as they're issued.

    c. Heed credible security warnings and move quickly to fix them.

10. **Secure paper, physical media, and devices.**

    a. Securely store sensitive paper files.

    b. Protect devices that process personal information.

    c. Keep safety standards in place when data is in route. (eg. When sending files, drives, disks, etc., use a mailing method that lets you track where the package is.)

    d. Monitor activity on your network.

Sourced from "Start with Security – Lessons Learned from FTC Cases" the FTC - ftc.gov/

Revised 06/07/21 BL

THIS CONTENT IS PROVIDED FOR GENERAL INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE ANY ADVICE WHATSOEVER, INCLUDING BUT NOT LIMITED TO LEGAL ADVICE OR TAX ADVICE. THE INFORMATION MIGHT NOT BE UP-TO-DATE, COMPLETE, OR ACCURATE, SO PLEASE UNDERTAKE DUE DILIGENCE, INCLUDING TALKING WITH A QUALIFIED LAWYER, CPA, OR OTHER PROFESSIONAL.