Getting Started with the NIST Privacy Framework: A Guide for Small and Medium Businesses

What is the NIST Privacy Framework, and how can my organization use it?

The NIST Privacy Framework[1] is a voluntary tool that can help your organization create or improve a privacy program. Effective privacy risk management can help you build trust in your products and services, communicate better about your privacy practices, and meet your compliance obligations. Good cybersecurity is important, but can't address all privacy risks.

Get started using the Privacy Framework by following a simple model of "Ready, Set, Go" phases, and align your business or agency with five privacy risk management areas: Identify, Govern, Control, Communicate, and Protect.

01 READY...

Get ready to create or improve your privacy program by using the Privacy Framework to build a strong foundation for identifying and managing privacy risks.

"It is difficult to make the case to build a privacy program ... the NIST Privacy Framework has been one of the tools we've been able to use, even when we're not able to staff a large privacy team."

JAIME LEES
CHIEF DATA OFFICER
ARLINGTON COUNTY GOVERNMENT

Identify:

- Identify the data you are processing (such as collecting, using, sharing, storing) and map out its flow through your systems throughout the full data lifecycle – from collection to disposal. This doesn't have to be comprehensive, especially at first, but it's a foundation for understanding your privacy risks.
- Conduct a privacy risk assessment[2] by using your data map to assess how your data processing activities could create problems for individuals (like embarrassment, discrimination, or economic loss). Then assess the impacts to your organization if those problems occurred (like loss of customer trust or reputational harm) that can negatively affect your bottom line.
- Ask about options for contracts and the products and services you use to run your business to ensure that they are set up to reflect your privacy priorities.

Govern:

- Privacy culture starts at the top. Determine which privacy values (for example, autonomy, anonymity, dignity, transparency, data control) your organization is focused on. Connect your organization's privacy values and policies with your privacy risk assessment to foster trust in your products and services.
- Know your privacy-related legal obligations so that you can build compliant products and services.
- Help your workforce know their roles and responsibilities so that they can make better decisions about how to effectively manage privacy risks in the design and deployment of your products and services.
- Regularly reassess to see if your privacy risks have changed. This can happen when you make improvements to your products and services, change your data processing, or learn about new legal obligations.

[1] https://www.nist.gov/privacy-framework
[2] https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

02

SET...

Now that you know your privacy risks and legal obligations and have a governance structure, your organization can focus on the policies and technical capabilities for your systems, products, and services.

Control:

- Are you collecting, sharing, or keeping data that you don't need? Consider how your policies help you or other organizations maintain control over data and how individuals might have a role as well.
- Take your privacy risks and legal obligations into account when deciding on the functionality of your systems, products, or services. Consider flexible design so that you can respond more cost-effectively to shifting customer privacy preferences and a dynamic legal environment.
- What kinds of data processing do you do? The more you can disassociate data from individuals and devices, the greater the privacy gains. Consider how different technical measures such as de-identification, decentralized data processing, or other techniques could allow you to meet your business or agency objectives while protecting privacy.

Protect:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of data and old devices.

"If you need to establish a privacy program, the NIST Privacy Framework is a perfect place to start."

JEEWON SERRATO
PARTNER
BAKERHOSTETLER

"The Privacy Framework can be a market differentiator for the organization to be able to grow their business."

MARY N. CHANEY, ESQ., CISSP, CIPP
DIRECTOR OF INFORMATION SECURITY AND PRIVACY
ESPERION THERAPEUTICS, INC.

Communicate:

- Craft policies for communicating internally and externally about your data processing activities.
- Increase transparency and customer understanding by providing clear and accessible notices and reports or implementing alerts, nudges, or other signals to inform individuals about your data processing activities and their choices.
- Do you conduct surveys or focus groups to inform your product or service design? Include privacy so that you learn more about customer privacy preferences.
- Consider what you will do in case of a data breach. How will you provide notifications or any remedies such as credit monitoring or freezes?

03

GO!

Now it's time to get from where you are today to where you want to be.

- How does your program stack up to what we've suggested here?
- Prioritize your target outcomes and create an action plan.
- Discuss your plan as an organization and use it to work towards acquiring the resources and building the workforce necessary to meet your goals.
- Put your plan into action! You're on your way to creating more trust in your products and services, communicating more effectively about privacy with your partners and customers, and meeting your compliance obligations!

NIST National Institute of Standards and Technology
U.S. Department of Commerce