

## PRIVACY AND COOKIE POLICY

---

### FireEye Online Privacy Statement

FireEye respects your privacy. When using our website, you may get information, communicate with us, or link to other websites with whom we do business. While doing this, you may give us information so that we can provide enhanced products or services to you, as well as personalize your experience on our website. This online privacy policy describes how FireEye, and its affiliates and subsidiaries use and protect Personal Information that you share with us. "Personal Information" is information that enables us to identify you. Examples of this kind of information include your email address, name, title, or mailing address, and there are other similar kinds of information that may be used for the same purpose.

Your privacy, and the privacy of all users of [www.fireeye.com](http://www.fireeye.com), is of the highest priority. If you have any questions, [please email us](#).

This policy governs websites owned and operated by FireEye. Our policy does not govern websites of other parties to which we may provide links because FireEye is not responsible for and cannot control the privacy practices or content of those sites.

Here are the principles governing our information practices and other privacy aspects of our websites:

- Information Collection and Use
- Information Sharing and Disclosure
- Cross-Border Transfer
- IP Information Collection and Use Practices
- Cookies
- Data Storage and Security
- Your Data Privacy Rights Dispute Resolution
- Contact Us
- Policy Updates

### Information Collection and Use

FireEye collects Personal Information when you register for FireEye information such as whitepapers and reports, newsletters or webcasts, visit FireEye pages, and enter promotions. This Personal Information may include your name, email address, and telephone number.

FireEye may collect any additional information relating to you that you voluntarily provide to us directly through our websites or indirectly through our representatives or business partners.

FireEye may use Personal Information received from you in connection with to fulfill your requests for information on products and services or any specific questions sent to us, to respond to any complaints, to contact you about offers and new products, to follow up on marketing initiatives and to generally manage your relationship with us.

### Information Sharing and Disclosure

FireEye will not sell or rent your Personal Information to anyone.

FireEye will send Personal Information about you to other companies or people when:

- We have your consent to share the information;

- We need to share your information to provide the product or service you have requested; We need to send the information to companies who work on behalf of FireEye (e.g., affiliates, distributors or resellers) to provide a product or service to you or for further follow-up related to your interests. The information shared does not constitute a sale of your Personal Information;
- We have to disclose your Personal Information in response to a lawful request by public authorities and agencies, to meet any applicable law and regulation or to protect FireEye's assets as permitted by law; or
- We are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). We may be required to disclose personal information that we handle under the Privacy Shield in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

### Cross-Border Transfer

FireEye may process or otherwise transfer any personal information in or to any country outside of the country of origination, including such countries with less restrictive data protection laws, to the extent necessary for purposes described in this policy. FireEye has entered into the [EU Standard Contractual Clauses](#) as approved by the European Commission, to help ensure an adequate level of data protection for any personal data that will be processed or transferred.

### IP Information Collection and Use Practices

- FireEye receives IP addresses from all users because this information is automatically reported by your browser each time you view a Web page.
- When a FireEye Web page is requested and viewed, that request is logged on our servers with information
- including the IP address of the computer that requested the page.
- IP addresses may be used for various purposes, including estimating the total number of users visiting FireEye from specific countries or regions of the world.

### Cookies

A cookie is a small amount of data, which often includes an anonymous unique identifier, that is sent to your browser from a website's computers and is stored on your computer's hard drive.

Each website can send its own cookie to your browser if your browser's preferences allow it, but to protect your privacy, your browser only permits a website to access the cookies it has already sent to you, not the cookies sent to you by other sites.

**FireEye Practices Regarding Cookies:** FireEye uses cookies for a number of purposes, including to:

- Provide you with customized content.
- Keep track of preferences you specify while you are using FireEye's products and services. Estimate and report our total audience size and traffic.
- Conduct research to improve FireEye content and services.
- Require you to reenter your FireEye password after a certain period of time has elapsed to protect you.

In addition to the first-party cookies we set, we use external services that set third-party cookies to:

- Enable information sharing across social media services.
- Provide you with targeted advertising in relevant contexts on external sites.

- Keep track of preferences you specify while you are using third-party services.
- Enable third parties to aggregate anonymous user behavior data and provide such research data to FireEye.
- Monitor and report on site and service usage across FireEye websites.
- Query third-party services such as Twitter for recently changed information.

**Similar Technologies We Use:** In addition to cookies, we use Web beacons (also known as "clear GIFs" and "1x1" pixels) and coded URLs. These techniques may be used:

- In online advertising to determine which advertisements you have viewed.
- In our promotional emails to track whether an email has been viewed and subsequent clicks on hyperlinks.
- To support remarketing for AdWords Ads on the Google Display Network. Remarketing technology serves you ads across multiple websites based on your browsing interest and behavior.

In addition, you may choose not to open emails or download images in emails you receive from FireEye.

To opt out of tracking via coded URLs, you may choose not to click on hyperlinks embedded in marketing emails you receive from FireEye.

## **Data Storage and Security**

### **Account Information:**

- When you submit information to FireEye, a temporary copy of that information is routinely made to prevent accidental loss of your information through a computer malfunction or human error.
- Please note that any information that we have copied may remain in back-up storage for some period of time after your deletion request. This may be the case even though no information about your account remains in our active user databases.
- FireEye does not react to Do Not Track signals because there is no standard for how those signals are sent.

### **Servers:**

- The FireEye computers (called "servers") that send your Web pages process and store an enormous amount of information every day. These computer records are called "log files."
- Log files are used for analysis, research, auditing, and other purposes, as described above. After this information has been used, it is stored and is inaccessible. Until the information is stored, your FireEye ID may remain in our active server log files.

### **Security:**

- Appropriate technical and physical safeguard measures are in place to protect against unauthorized or unlawful access, misuse, accidental loss, destruction and alternation of any Personal Information which are shared with us in the course of using our website services.

## **Your Data Privacy Rights**

You have a number of rights under relevant data privacy laws, which may include the General Data Protection Regulation (EU) 2016/679 and the California Consumer Privacy Act. Depending on where you are based, those rights may include the right to (i) request access or copies of your personal data FireEye processes, (ii) rectify incorrect personal data, (iii) delete your personal data, (iv) restrict the processing of your personal data, (v) determine the portability of your personal data, (vi) lodge complaints with competent authorities in your country, and/or (vii) request a list with the names and addresses of any

potential recipients of your personal data. To exercise one or more of these rights, or to ask questions or relay concerns, please contact FireEye's Data Protection Officer:

Richard Weaver  
FireEye Security Holdings US LLC  
11955 Freedom Drive, Suite 300  
Reston, Virginia 20190, USA  
(703) 935-8012  
[privacy@fireeye.com](mailto:privacy@fireeye.com)

FireEye will verify requests that it receives and respond in the time period required under the relevant data privacy laws.

### **Dispute Resolution**

If you believe your Personal Information has been used in a way that is not consistent with this Policy, we invite you to contact FireEye first at [privacy@fireeye.com](mailto:privacy@fireeye.com). We will make all efforts to resolve your complaints in a timely and accurate manner.

### **Contact Us**

If you have any questions about this privacy statement, the practices of this site, or your dealings with this website, [please contact us](#).

### **Policy Updates**

We may update our Policy from time to time. We will post the updated version in this section of the website. If the revision is significant and may materially change our data privacy practices, we will notify you by using other means, e.g., via email.