OBJECT
FIRST

CISA Secure by Design Pledge

Object First Reinforces its Commitment

What is Secure by Design?

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

It collaborates with stakeholders in industry and government to strengthen their own security and resilience. As part of its efforts, CISA has developed the **Secure by Design Pledge**. This pledge encourages software manufacturers to voluntarily enhance the security of their enterprise software products and services. The pledge is structured around seven goals, each with core criteria manufacturers commit to achieving.

Manufacturers are encouraged to demonstrate measurable progress towards these goals across all their products and to communicate goal completion or a roadmap to completion.
If a manufacturer meets or exceeds a goal, they are encouraged to describe their actions publicly.

This pledge complements and builds on existing software security best practices developed by CISA, NIST, other federal agencies, and international and industry best practices. It aims to advance a ‘secure by design’ posture in the software industry.

Object First is proud to sign CISA’s Secure by Design pledge. Our flagship product, Ootbi, currently meets or is in development to complete the pledge’s criteria.

We believe it is vital that all vendors do the same. This document will highlight our progress towards meeting the Secure by Design Pledge criteria.

Multi-Factor Authentication (MFA)

CISA's Goal

> Within one year of signing the pledge, demonstrate actions taken to measurably increase the use of multi-factorauthentication across the manufacturer's products.

Object First Pledges

Object First meets this goal today. Object First Ootbi supports MFA configuration, and our best practices describe configuring this as part of the initial setup and configuration. MFA can be enabled via the settings module within our product web user interface.

Default Passwords

CISA's Goal

> Within one year of signing the pledge, demonstrate measurable progress towards reducing default passwords across the manufacturers' products.

Object First Pledges

Object First meets this goal today. One password is used during the initial configuration, uniquely generated per appliance, and printed on the pullout tab for connecting via IPMI. Upon configuration, the user is prompted to create a strong password for all future logins. No universal default passwords are used.

Reducing Entire Classes of Vulnerability

CISA's Goal

> Within one year of signing the pledge, demonstrate actions taken towards enabling a significant measurable reduction in the prevalence of one or more vulnerability classes across the manufacturer's products.

Object First Pledges

Object First contracts with third party testing agencies to perform penetrative testing to help find and remedy security gaps. For example, during testing in Q2 2024, we identified some gaps during testing and released an interim Ootbi 1.5 patch to address them.

Security Patches

CISA's Goal

> Within one year of signing the pledge, demonstrate actions taken to measurably increase the installation of security patches by customers.

Object First Pledges

Object First meets this goal today. Object First continuously releases product patches that address customer feedback and security findings. When updates are available, we notify customers directly through the product UI if they are on a previous version. We aim to ensure all customers are on the latest version when possible, but we also acknowledge that, realistically, this can not always be monitored or enforced, so we have set a goal for all Object First customers to be on the latest security patch within 30 days of release.

We will implement a process to help increase security patch adoption by evaluating current customer product versions via product telemetry collection and then orchestrating a multi-step follow-up program through the Object First Customer Success Team that will help inform and encourage update adoption.

Vulnerability Disclosure Policy

CISA's Goal

> Within one year of signing the pledge, publish a vulnerability disclosure policy (VDP) that authorizes testing by members of the public on products offered by the manufacturer, commits to not recommending or pursuing legal action against anyone engaging in good faith efforts to follow the VDP, provides a clear channel to report vulnerabilities, and allows for public disclosure of vulnerabilities in line with coordinated vulnerability disclosure best practices and international standards.

Object First Pledges

Object First meets this goal today. Object First's vulnerability disclosure policy is available to review on our website at:
https://objectfirst.com/legal/vulnerability-disclosure-policy/

Anyone who has identified a security concern can contact us directly through email at **security@objectfirst.com.**

CVEs

CISA’s Goal

Within one year of signing the pledge, demonstrate transparency in vulnerability reporting by including accurate Common Weakness Enumeration (CWE) and Common Platform Enumeration (CPE) fields in every Common Vulnerabilities and Exposures (CVE) record for the manufacturer’s products. Additionally, issue CVEs in a timely manner for, at minimum, all critical or high impact vulnerabilities (whether discovered internally or by a third party) that either require actions by a customer to patch or have evidence of active exploitation.

While not required for this goal, companies are encouraged to go above and beyond by filing CVEs for other vulnerabilities that do not meet these criteria for the reasons described below. Companies are also encouraged to explore additional ways to enrich their CVE records to help customers better respond to vulnerabilities.

Object First Pledges

Object First will publish a report of any Common Vulnerabilities and Exposures (CVEs) in 2024.

Evidence of Intrusions

CISA’s Goal

Within one year of signing the pledge, demonstrate a measurable increase in the ability for customers to gather evidence of cybersecurity intrusions affecting the manufacturer’s products.

Object First Pledges

Object First meets this goal today. Object First Ootbi’s audit logs and support bundles allow users to package and send any reports to us directly and efficiently. They may also make a report through the previously mentioned VDP or by emailing **security@objectfirst.com.**

Learn More

Veeam customers deserve a solution that is secure by design and prioritizes data resilience. Visit Object First to learn how Ootbi (Out-of-the-Box Immutability) provides a secure, simple, and powerful backup storage solution that best protects Veeam backup data against insider threats, cyberattacks, and ransomware.