Understanding Security and Compliance Policies

https://campus.barracuda.com/doc/80740643/

This article provides background on each of the policies available in Barracuda Cloud Security Guardian. For details on implementing these policies in Barracuda Cloud Security Guardian, refer to Assigning a Security Policy to a Cloud Connection.

Barracuda Cloud Security Guardian includes the following policies to protect your cloud infrastructure:

- CIS
- PCI DSS
- HIPAA
- NIST
- Barracuda Security Best Practices

The Default Policy shipped with Barracuda Cloud Security Guardian includes *all* of the policies to ensure that you are covered from the most threats. Depending on your organization and your uses, you might only want to use some of these policies, so you can create your own custom policies. For more information, refer to Assigning a Security Policy to a Cloud Connection.

CIS (Center for Internet Security)

The Center for Internet Security is a non-profit entity for safeguarding organizations against cyber threats. According to its website (https://www.cisecurity.org/about-us/):

"The CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals."

For additional information, refer to https://www.cisecurity.org/.

PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS is an industry standard for organizations that process credit cards. The standard is required by major credit card brands and is administrated by the Payment Card Industry Security Standards Council.

For additional information, refer to https://www.pcisecuritystandards.org/.

HIPAA (Health Insurance Portability and Accountability Act)

The Health Insurance Portability and Accountability Act of 1996, gives patients in the United States rights over their health information and sets rules and limits on who can look at and receive health information. The Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral. The Security Rule is a Federal law that requires security for health information in electronic form.

For additional information, refer to https://www.hhs.gov/hipaa/index.html.

NIST (National Institute of Standards and Technology)

The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce. NIST handles many different kinds of standards. Here we are concerned with the National Vulnerability Database. According to the NIST website, this database includes "databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics."

For additional information, refer to https://nvd.nist.gov/.

Barracuda Security Best Practices

Barracuda considers the following practices to be critical. Assign these policies to your cloud connections as you would the other policies described on this page.

- Web applications should be protected by a web application firewall
- Email domains should be protected by an email security solution