BELLESBOARD

SECURITY

HOW DOES BELLESBOARD APPROACH SECURITY?

BellesBoard provides a multifaceted defense to protect your board information and documents. We take security seriously and follow **OWASP (Open Web Application Security Project) best practices**. BellesBoard is also **AICPA and SSAE Certified**. With BellesBoard, your organization will have the peace of mind to know that your information and documents are safe and secure.

SECURITY OVERVIEW

PORTAL INFORMATION	• BellesBoard enforces HTTPS connections. A 256bit SSL certificate is used to ensure an encrypted connection from the user's computer to BellesBoard. • Passwords are one way encrypted and strong passwords are enforced. • Unique account per user.
WEB APPLICATION FIREWALL	• BellesBoard's hosting uses redundant firewalls that provide for intrusion prevention and detection. • BellesBoard firewalls use deep packet inspection. • Firewall rules are updated hourly by a third party service. • Web application firewalls are also used. • BellesBoard code is hardened against attacks such as SQL injection attacks and cross-site scripting attacks.
DATA & HOSTING	• Data is backed up daily. • Our managed hosting provider performs nightly third party security audits. • Our host blocks access to all non-common ports. • The data belongs to the Client, as stated in the BellesBoard Master Agreement.
PORTAL MAINTENANCE	• All patches are applied in off hours and • customers are notified prior to the patches being applied. • All patches are tested before applying to production servers. • Production servers are backed up before applying patches.