Brivo Onair Security and Compliance Customer Overview

January 2020

brivo

Legal Disclaimer

Documentation Disclaimer and Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Brivo Systems LLC. For the most up-to-date information, visit www.brivo.com.

This document and the data herein shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized with the written permission of Brivo Systems LLC. The information contained within this document or within the product itself is considered the exclusive property of Brivo Systems LLC. All information in this document or within the hardware and software products themselves is protected by the copyright and/or other intellectual property laws of the United States.

Table of Contents

Legal Disclaimer 2
Table of Contents 3
Introduction 4
- Assumptions 4

Onair Architecture 5
- Onair Account Management 6
- Access Control Panels 6
- Access Control Process 6
- Video Services 7
- API Services 7

Cloud Computing Security 7
- Resilient Design 7
- Continuous Monitoring 8
- Vulnerability Scanning 8
- System Maintenance/Patching 8
- Multi-Tenancy 8

Network Security 8
- Web Application Firewall (WAF) 8
- Intrusion Detection System (IDS) 8
- Headquarters Office Network 8
- VPN 9

Access Control Panel Security 9
- Data at rest 9
- Networking 9
- Bot Detection 9
- Data in motion 9
- Panel Administration Interface 10

Onair Security Features 10
- Administrator Authentication 10
- Logging & Reporting 10
- TLS 10
- Cookies & Sessions 10

Software Development Life Cycle (SDLC) Security 11
- Secure Development 11
- Change Control Process 11
- Application Vulnerability Scanning 11
- Penetration Testing 11

Mobile Applications Security 12
- Brivo Onair Mobile Application 12
- Brivo Mobile Pass 12

Security Policies 12
- Risk Management 12
- Supply Chain Risk Management 12
- Access Control 13
- Security Training 13

Physical Security 13
- Visitors 13

Privacy 14
- EU Citizens 14
- Privacy Contact Information 14

Additional References 14

Introduction

As a provider of physical security services, we at Brivo believe that information security is of paramount importance to maintaining the safety and security of your facilities, and the privacy of your data. That's why information security has been a consideration since day one.

Brivo looks at security holistically in our technology, people and processes. We use guidance from industry best practices, applicable publications, and international regulatory requirements to employ a defense-in-depth strategy for the controls in our security framework.

Assumptions

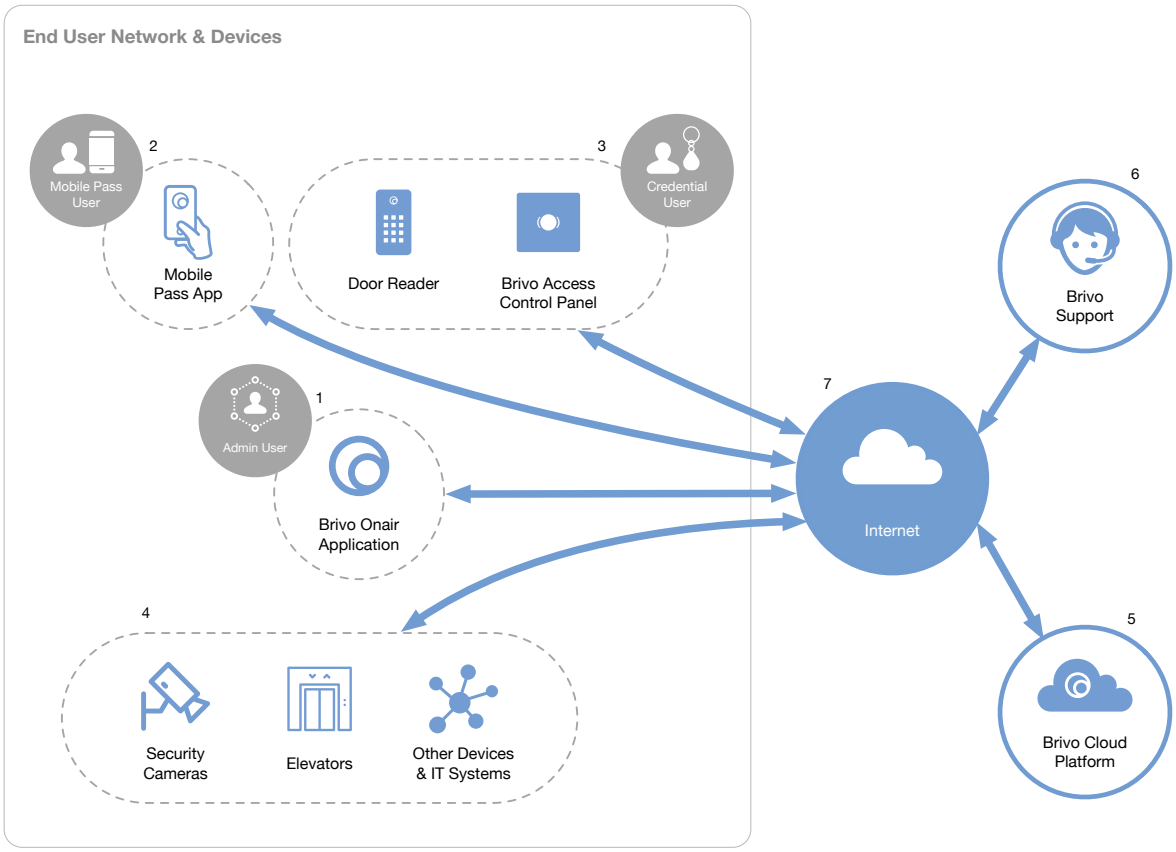
Some security features in this paper are not available on outdated hardware or firmware, this paper will call out those features so that users can request hardware and firmware updates. To check your panel firmware, log into your Onair account and navigate to the Setup > Control Panels screen. If your panel needs a hardware or firmware update, contact your Brivo authorized reseller.

This paper is primarily intended for IT professionals familiar with computer networks and information security.

Onair Architecture

Brivo Onair is a physical security Software as a Service (SaaS) primarily targeted at commercial and multi-unit residential properties with employee, resident, and visitor populations for whom access needs to be regulated and recorded. A cloud hosted system such as Onair is an excellent fit for geographically distributed applications that span multiple properties.

Figure 1: Brivo System Overview



As shown above in Figure 1, there are seven major components to the operation of the Brivo Onair® service:

1. Brivo Onair application (available via web browser or mobile application)
2. Brivo Mobile Pass credentials (optional)
3. Access control hardware installed on customer network used with physical credentials
4. Connections to other devices and IT systems
5. Brivo services are hosted with major cloud service providers
6. Brivo employees providing support, maintenance, and continuous monitoring.
7. Network communications via Internet.

These components share data across multiple platforms and networks in order to manage access control privileges, deliver alarm and event records and to provide other services such as software updates to control panels.

Control panels are networked to the cloud through wired or wireless connection. Wired options include a built-in Ethernet port for connection to a corporate LAN, or broadband modem, or any other IP-based networking technology with connectivity to the Internet. Wireless networking options include a cellular network router or wi-fi adapter that comes with or is built into the control panel.

Onair Account Management

The access control life cycle begins with an administrator logging into the Brivo Onair application (web-browser or mobile application) and setting up users, groups, credentials, schedules, and other security policy elements that dictate who has permission to enter which facilities at which times. Any activity in an Onair account performed by an administrator is logged in the journal report.

Administrators can also issue Brivo Mobile Pass credentials to users. The user will need to install and activate the Brivo Mobile Pass application on their mobile device, then they can use either a bluetooth connection, or an Internet connection to unlock the door(s) that they have permission to (depends on the reader hardware).

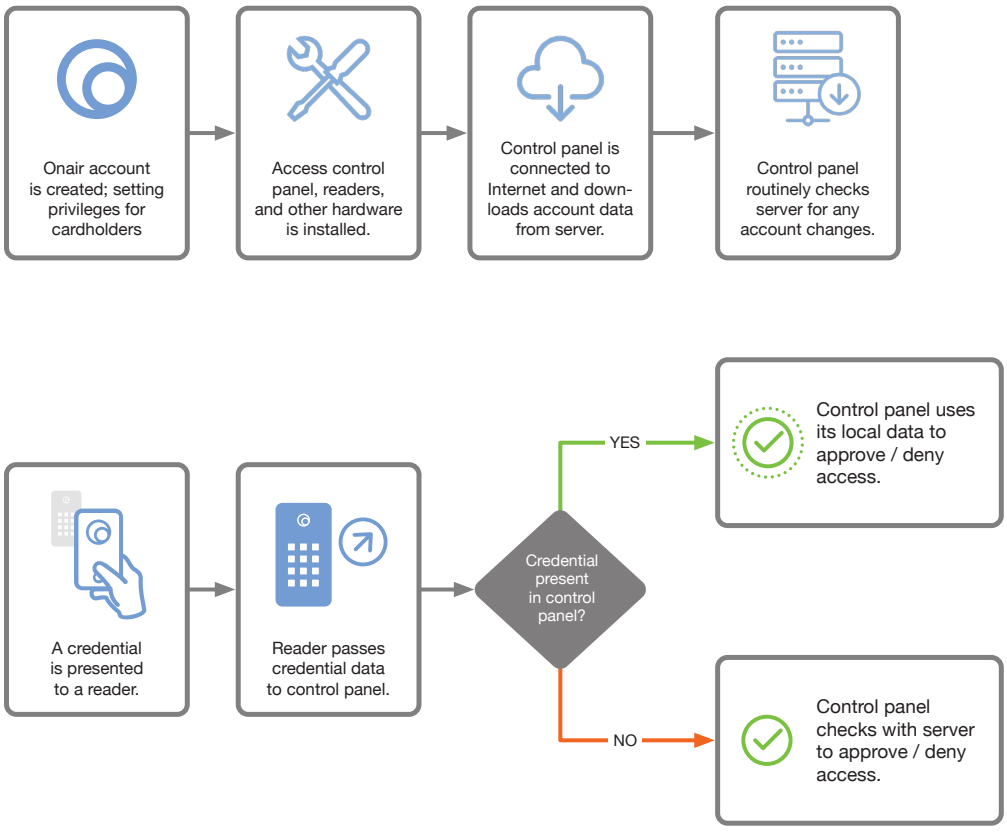
Access Control Panels

Administrators can also issue Brivo Mobile Pass credentials to users. The user will need to install and activate the Brivo Mobile Pass application on their mobile device, then they can use either a bluetooth connection, or an Internet connection to unlock the door(s) that they have permission to (depends on the reader hardware). An access control panel is hardware installed by a Brivo authorized reseller on the customer's premises. This panel is the interface between Brivo's cloud platform and physical devices on premise such as credential readers, door locks, request-to-exit motion sensors, and exit buttons. The Brivo access control panel's primary function are to keep doors locked until a user presents an authorized credential at a reader and to monitor doors for any unauthorized openings.

The account data is stored in Brivo's cloud data platform. The control panel, upon initial connection, will download the data file to approve or deny users as the administrator has programed. The panel will establish a connection channel with the server and check regularly for new account data. If changes are made to doors in the Onair account, an update is pushed to the panel from the server using the pre-existing channel or upon the next panel connection.

Access Control Process

Figure 2: Data Flow for Access Events



When a credential is presented to a reader, the reader will send the card data as a hexadecimal value to the access control panel. The panel can make a local decision to unlock the door and will check with the host if the card data is not stored in the panel database. If the access request is not valid, access is denied and the panel will not unlock the door. The panel will update the activity log in the account with the event whether approved or denied.

In the event that the control panel loses an Internet connection, it will use a local cache of the account data that will allow the panel to operate based on it's last configuration. When connectivity is restored, the panel will request and download any changes to the account.

Video Services

Brivo Onair offers video hosting services. Internet connected security cameras installed by a Brivo authorized dealer on the customers' premises connect to Onair servers to stream live video and store video recordings (optional). Video communications are protected by TLS encryption in transit. Video cameras are connected on the customer's network and the administrative interface is protected by a username and randomly generated unique password. This password can be changed by the user. The password also changes to a new randomly generated password if the camera disconnects and reconnects to the server.

API Services

Brivo offers API services for third-party integrations. Brivo API uses OAuth2 three-legged authorization code workflow for account access. Account Administrators are provided the ability to selectively enable API connections to their Brivo Onair account. All communications via the API are HTTPS using TLS 1.2 or higher. For more technical information on Brivo API, visit our documentation (https://apidocs.brivo.com).

Cloud Computing Security

Brivo Onair is delivered as a multi-tenant model using secure logical controls to separate customer data. Brivo leverages AWS hosting services and other third party solutions for a secure and resilient solution. AWS has a comprehensive security program that Brivo evaluates continually as part of its supply chain risk management program. AWS publicly provides details on their security program and data centers which you can find on their website (https://aws.amazon.com) including:

1. AWS Security Overview
2. AWS Data Centers
3. AWS Compliance Programs

Brivo understands that by using AWS, we must maintain and secure our resources as part of the AWS shared responsibility model. Brivo implements a security program specific to these resources including access control, secure network configuration, continuous monitoring, firewalls, IDS and system configuration/patching. More details on how we do this will be covered in this paper.

Resilient Design

To provide high availability of our services, Brivo replicates services across three availability zones in AWS US-EAST-1 region located in Northern Virginia, United States. This enables Brivo to release updates to services seamlessly and to provide services in the event of an AWS availability zone outage. Backup snapshots are performed daily of our database. We maintain some resources in the AWS US-WEST-2 region located in Oregon, United States as a warm disaster recovery site. All data is stored within the contiguous United States.

Brivo believes in transparency as part of building trust with its users. We announce status updates for any planned or unplanned downtime publicly on our status page (https://status.brivo.com/).

Continuous Monitoring

Brivo has a suite of tools fine tuned by operations staff to monitor critical systems. These tools create baselines for system performance and alert staff when performance is abnormal. This could signal an upcoming service disruption, or a potential security event. We have staff on call 24/7 to respond to these alerts.

Vulnerability Scanning

Brivo uses a vulnerability scanning tool to assess our environment. This tool automatically scans systems every 24 hours and identifies any potential flaws in their configuration or installed operating system and services. The tool alerts our security and operations teams on new vulnerabilities for investigation and remediation.

System Maintenance/Patching

Brivo performs patching periodically in order to keep systems up to date and reduce vulnerabilities. In the event of a high risk patch identified by a security advisory or vulnerability scan, we create a mitigation plan, test the proposed mitigation non-production environment and if no issues arise, deploy those updates to production with no downtime.

Multi-Tenancy

Brivo logically separates customer accounts within the database. When an account is created, it is tied to a unique identifier that is hidden to the end-user. When any action is done on an account, the unique identifier and valid credentials are needed. Brivo Onair administrators can be granted different levels of privileges for reading, modifying, or deleting user groups or sites within the account.

Network Security

Brivo configures logical networks in AWS using built-in security features. Environments are logically separated through the use of different AWS accounts, security groups, and subnetting. Security groups are configured with a white list of ports and IPs to ensure that only the ports absolutely necessary for providing services are open. AWS provides secure network hardware and automatic encryption of all traffic on the AWS global and regional networks between AWS secured facilities.

Web Application Firewall (WAF)

Brivo uses a Web Application Firewall (WAF) in addition to the built in network security features to additionally monitor and restrict traffic flowing to AWS resources. The WAF is set up with rules to deny traffic that is from known bad reputation IP addresses.

Intrusion Detection System (IDS)

Brivo uses an AWS featured partner to provide an Intrusion Detection System (IDS), web application security event detection (passive WAF), security event log aggregation, and a team of security experts that provide 24x7x365 threat monitoring and tuning. These services alert the security and operations teams when any potential incidents such as suspicious network traffic is detected. Detection is both anomaly-based and signature-based. Potential incidents are investigated by the Brivo team to rule out false positives. All true positives are added to Access Control Lists (ACLs) in the WAF to block.

Headquarters Office Network

Brivo's headquarters network uses logical separation of departments through subnetting. The network firewall whitelists only the ports necessary to provide services. For resiliency, Brivo utilizes two different Internet providers. All necessary devices are connected to a battery backup and surge protection. Network devices are in a physically secured server room to prevent non-authorized employees or visitors from accessing devices. Brivo has backup

air conditioning in the event of HVAC failure. In the event of a disaster, employees are able to work from home to continue maintaining services and providing support to end users.

VPN

Brivo employees and contractors must use a Brivo-managed VPN to access network resources when remote and some sensitive systems when on location. Use of this VPN allows another layer of access control, logging, and encryption for employee network traffic.

Access Control Panel Security

A control panel is dedicated hardware containing a microprocessor, memory, and I/O interfaces that allow it to interconnect to credential input devices such as readers, and door control and sensor hardware such as latches and switches. Brivo has designed and manufactured several models of control panels which differ in capacity, communication options, and features.

Data at rest

Data at rest on the control panel is encrypted. The encryption method used is listed in the panel data sheet found on our website (www.brivo.com). For the new models at the time of writing (ACS300 or ACS6000) panels, the encryption method is AES256.

Networking

The Brivo control panel initiates all communication sessions with the Brivo server. The IP address assigned to the panel does not need to be a static or routable IP address. This means that the control panels will operate with routers and firewalls configured to use Network Address Translation (NAT).

Panels require outbound HTTPS traffic (TCP port 443) open to connect to Brivo servers. Panels will not accept inbound connections, they will only listen to network traffic within the HTTPS session which was initiated by the control panel itself. For networks with firewalls that whitelist IPs, Brivo Customer Care can provide a list of IPs required for our panels to communicate. To get the most updated whitelist, contact customercare@brivo.com. For networks with a proxy server, panels have built in support for the SOCKS 5 and HTTP proxy protocols.

Bot Detection

Brivo panels monitor their connections and are only permitted to connect to specific whitelisted IP addresses using specific service protocols. If at any time the panel is redirected to a non-Brivo server, the panel would not allow the connection and would alert the Brivo server. This is to prevent a process (bot), which was planted on a panel to create a cyber attack such as denial-of-service (DoS attack).

Data in motion

All control panels exchange credential and event information with the Brivo data center. Brivo uses digital certificates described by the ANSI X.509 specification for public key infrastructure (PKI) systems. For control panels, Brivo acts as its own CA because it can guarantee a physical chain of custody during the installation of certificates into control panels during our manufacturing process, and because there are no third parties communicating with those panels who need to be part of the authentication process.

Brivo control panels communicate via TLS1.2+ with AES 256-bit encryption and Digital Signature Algorithm (DSA) verified SHA256 digital certificate signed with a key length of either 1,024 or 4,096 bits, depending on the device. Panels establish a TLS session with Brivo before exchanging information. When establishing a TLS session, the panel

and the server validate each others' certificate to authenticate their identity.

Some older firmware or hardware models do not support these levels of encryption. Check the data sheet for your hardware model on the website (https://www.brivo.com) to confirm what your panel specifically is capable of. If unsure, check with your Brivo authorized reseller to confirm that you are on the latest firmware version and hardware model.

Panel Administration Interface

The panel administration interface (AKA Web CLI) is only accessible by a direct Ethernet connection to the panel. Panels should be installed in a secure location to prevent tampering with the hardware. The interface requires a username and password to access, this password can be changed. Data accessed in the interface are device settings such as networking configuration, amount of connected devices, and logs of activity that do not contain PII.

Onair Security Features

Administrator Authentication

An administrator is a Brivo Onair user with privileges to sign in to the Brivo Onair application and observe or make changes to an account that controls one or more sites. Brivo authenticates administrators by an administrator ID and password. Passwords may be between 8 and 128 characters in length and must contain at least 2 of the following 4 categories: Lower Case, Upper Case, Digit, and Non-Alphanumeric.

Brivo offers and recommends administrators to enable two-factor authentication on their account. This feature requires all administrators within an account to set up an email address to receive two-factor authentication token. Two-factor authentication tokens are valid for a limited time (5 minutes).

Administrators may set up a secret question and answer to receive a password reset via a self-service option on login screen. Brivo recommends using a randomly generated secret answer saved within a password manager when using any secret question and answer service.

Logging & Reporting

All administrator activity is logged in the Journal report in Onair. This includes activity when Brivo customer support is asked to log into an account to assist in troubleshooting. All access events (success or failure), video motion events, and other events are logged in the Activity log in Onair. Onair administrators with sufficient permissions can download their data by running reports. All data is retained per the Terms of Use for Brivo Onair (https://www.brivo.com/terms-of-use-brivo-onair/).

Encrypted Communications

Brivo Onair supports TLS 1.2+ connections and will negotiate that as long as the client web browser and operating system allows it.

Cookies & Sessions

Brivo Onair uses sticky sessions to maintain state information and provide a continuous experience to clients. To use sticky sessions, the clients must support cookies. Cookies have the secure flag enabled so they are transmitted via HTTPS and will not reveal session token data.

Onair will log out users once they have been inactive longer than 20 minutes unless the user is monitoring the real-time activity log.

Software Development Life Cycle (SLDC) Security

Brivo uses security best practices throughout the Software Development Life Cycle (SDLC). This means that security is included throughout phases of development and deployment.

Secure Development

Brivo engineers are provided secure development training curriculum specific to the programming language they use. Every engineer is required to complete their curriculum. This program trains on the OWASP Top 10 vulnerabilities and how to mitigate them through secure coding practices. Engineers have a plugin in their integrated development environment (IDE) to highlight security best practices or vulnerabilities that need to be remediated inline as they are writing code. Engineers can also create a sandbox on their machine to perform static application security scans on files they are working on so they can remediate any flaws before submitting a release for QA. The security team and management track the progress of training and results of sandbox scans.

Change Control Process

The development, QA and production environments are logically separated within the cloud. In order to submit any releases to QA or production environments, Brivo has a change control process to ensure that every release meets the criteria as set forth by management. This process requires every release to be ticketed with a release script that includes roll back procedures before submitting to QA environment.

Once in QA environment, the release is tested through tools and manual input. Those results and the release script must be approved by an engineering director in a change review meeting prior to being released to production. Releasing to production generally does not cause any outage of services due to the resilient design of our environment, however if any outage is planned, our Status Page (https://status.brivo.com) will be updated with a maintenance notification 24 hours prior to the release. Once deployed, regression testing is performed. If there is any disruption to customer experience, then the release is rolled back for investigation.

Application Vulnerability Scanning

Brivo is listed in the Veracode verified directory for Brivo Onair. We use Veracode static analysis, dynamic analysis, and source component analysis to identify any vulnerabilities within Onair, Partner Portal and API services.

Static analysis is done automatically with every build of our applications. Static analysis tests the application's source code for any vulnerabilities including OWASP Top 10, CIS Security Controls, etc.

Dynamic analysis is done weekly in production. Dynamic analysis is an automated test that crawls through the website to determine if it can identify or exploit any vulnerabilities.

Source component analysis reviews the usage of third-party libraries to check their licensing, determine if any are out of date, or determine if any have any known vulnerabilities.

Penetration Testing

Brivo has contracted a well established third-party provider to conduct annual penetration tests. These tests aim to discover vulnerabilities and exploit these vulnerabilities to gain unauthorized access to data or systems. Any results received are prioritized by our engineering teams for remediation and followup testing is performed by the third-party provider. The goal is to have no vulnerabilities after remediation.

Mobile Applications Security

Brivo Onair Mobile Application

The Brivo Onair mobile application is designed to allow administrators to view their activity, update user permissions, view live video, or unlock a door from their mobile device. The application authenticates the user through the same means as the Onair web application. Activity in the Onair mobile application is logged in the same way as the Onair account. Administrators also have the same level of permissions in the application as they would in their Onair account.

Brivo Mobile Pass

The Brivo Mobile Pass application is an optional virtual credential for card holders (users) to access doors. When this credential type is assigned to a user by an administrator in Brivo Onair, they must enter a valid email address. The user will receive an email to activate the application on their phone. The phone can connect to Bluetooth readers or can connect over an Internet connection to the Brivo server to send an unlock command. The mobile app will operate doors to which the user has valid, active permissions. The mobile app also has a built-in Digital Badge containing user photos uploaded to Onair via one of the administrative applications (web browser or mobile application). The digital badge contains a real time security feature to guard against the use of static screen shots of valid badges.

Brivo recommends enabling additional features in the Onair account regarding the Pass application.

- **Biometrics**: Requires user to authenticate using the mobile device's built in biometric or code based challenges to access doors. This setting can be enabled on each door.
- **Trusted Network**: Require the mobile device to be connected to a designated trusted wi-fi network prior to unlocking doors. This prevents accidental use by users when not on the trusted network, such as from home. This setting is enabled for the entire site.
- **Bluetooth**: The bluetooth option is requires close proximity to the reader to function. This setting can be enabled on each door and requires bluetooth capable door readers.

Security Policies

Brivo has an array of security policies as approved by an internal Information Security Team (IST) including members of senior management. These security policies are based on best practices and are audited by a third-party annually as part of our SOC 2 assessments. Our latest SOC 2 report can be requested from our Sales team (sales@brivo.com) and provided under mutual NDA. The IST and managers are responsible for assessing compliance to these policies and identifying risks. The team meets monthly to discuss security governance. If any risks are identified, the IST will report those risks to the Risk Management Committee (RMC).

Risk Management

The IST reports risks to the Risk Management Committee (RMC) at least quarterly. The RMC is comprised of the executive leadership team and are responsible for making any business decisions in regards to risk. Annually, the RMC review an organization risk assessment together that assesses the entire organization for risk.

Supply Chain Risk Management

Brivo uses an IT supplier policy to govern the selection and analysis of vendors in the supply chain. Any vendors that may have access to sensitive data are assessed for security best practices. The security team will review the

documentation for the vendor such as audit reports, white papers and any other security-related material the vendor provides annually. If any concerns are identified, then the security team reaches out to the vendor for remediation.

Access Control

The Brivo policy around access control requires access to be granted using role based and least privilege principles. Prior to granting any access, Brivo employees are screened in an interview process and undergo a background check. Sensitive systems access is reviewed quarterly by the IST to prevent access creep. Access is revoked immediately upon termination. Brivo requires the use of two-factor authentication and single-sign on where available.

The password policy requires passwords to be at least 8 characters in length and must contain at least 2 of the following 4 categories: Lower Case, Upper Case, Digit, Non-Alphanumeric. Password hygiene training is available for all employees and included in security awareness training. Brivo system administrators are required to change default passwords on all systems to passwords that meet the requirements in this policy.

Customer support teams perform authentication for callers using probing questions and/or an email from the account on file to verify the caller identity prior to performing any actions on an account.

Security Training

Brivo has several security trainings for employees including targeted role-based training and a security awareness program for all employees that is taken during onboarding and annually thereafter. The Security Awareness program for new employees is a classroom type session and includes, but is not limited to, password hygiene, how to identify a social engineering attack, data classification and information handling, and how to report any security events. The training is updated annually and delivered annually via a training system with a test to assess comprehension.

Brivo provides supplemental role-based training for our Sales, Marketing, Engineering, and Customer Care teams. These teams have different security responsibilities such as secure development, account handling and customer data. These trainings include senior management and are held in a classroom setting.

Physical Security

Brivo headquarters, located in Bethesda, MD, USA, is secured at the building and office level with access control systems. Brivo employees are granted access control cards with the minimum access needed to perform their duties. Brivo uses difficult to reproduce smart cards to access secured areas. Cameras are installed in the office and monitored for all access points and secured areas. Security guards monitor and patrol the building and surrounding premises.

Visitors

Visitors are required to sign in and are not granted access to office areas unless escorted by an authorized Brivo employee. Visitors are granted unique visitor badges which they must have visible on their person while on the premises. These badges are returned when they leave.

Privacy

Brivo values the privacy of our end users and we are transparent with our privacy policy. For our privacy policy in regards to business practices and the use of the Brivo website, please review our Privacy Policy as found on our website (www.brivo.com/privacy/). For the specific privacy policy surrounding the use of Brivo Onair services, please see our Services Privacy Statement as found on our website (https://www.brivo.com/services-privacy/). l

EU Citizens

Brivo complies with the requirements in GDPR and the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Our Privacy Shield listing is available to the public for review on the Privacy Shield website (https://www.privacyshield.gov/).

Brivo has entered into a number of Data Processing Agreements that include the EU standard contractual clauses in accordance with Article 26(2) of Directive 95/46/EC of the GDPR.

Privacy Contact Information

If you have questions regarding Brivo Privacy Policies or if you need to request access to or update, change or removal of personal information that we control, you can do so by contacting:

Brivo Privacy Officer
Brivo Systems LLC
7700 Old Georgetown Road, Suite 300
Bethesda MD, 20814 USA
privacy@brivo.com
+1 301-664-5277

Additional References

While this paper is intended to be a stand-alone document, you may have additional interest in either the Brivo system or some aspects of information security discussed. For that reason, a brief list of supplemental Brivo references are provided below.

- Brivo Onair Administrator's Manual
- Brivo Control Panel Installation Manual
- Brivo Product Data Sheets

These reference documents and more are available on our website (www.brivo.com). You may send any security questionnaires or requests for information to our sales team (sales@brivo.com).