SECURITY WHITEPAPER

CONTENT

Introduction

BlueCard has an existential interest in protecting your data.

That's why being worthy of your trust and the security of your data are our highest priorities. It's also why we're dedicated to ensuring that your information is always secure and only used for the purposes described in our privacy policy.

We take comprehensive measures to (i) protect our infrastructure, network, and applications; (ii) train employees in security and privacy practices; (iii) build a culture where being worthy of trust is the highest priority; and (iv) put our systems and practices through rigorous third-party testing and auditing and monitor compliance 24/7 to ensure ourselves and our customers that our security controls and practices are working as intended.

Our robust security management program has over 100 controls and focuses on security governance, risk management, and compliance and is aligned with global security standards and frameworks, like ISO 27001, AICPA SOC Trust Service Principles, and NIST standards, and is constantly evolving with updated guidance and new industry best practices.

BlueCard is SOC 2 Type II and HIPAA compliant and satisfies the vendor obligations imposed by FERPA.

Type II

FERPA

HIPAA

Application Security

BlueCard is designed with multiple layers of protection, with a strong emphasis on secure data transfer. This is accomplished through the use of modern data encryption standards, network security, server hardening, vulnerability management, administrative access control, system monitoring, logging and alerting, and application-level controls, all distributed across a scalable, reliable, and secure infrastructure.

Our approach to security is based on a zero-trust security model, meaning our organization does not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to our systems before granting access.

Authentication

All authentication to the BlueCard system occurs over secure channels and we offer multiple identity management methods.

Email

Users can sign up directly using their email and a password of their choosing. We enforce a strong password policy on all users and prompt users to change their passwords every 90 days. To protect the login credentials of users that sign up with email, passwords are hashed, salted, and then iteratively hashed again in order to increase the amount of time it would take to brute-force a password making it virtually impossible with modern technology. These practices also help protect against dictionary and rainbow table attacks. As an added precaution, we encrypt the hashes with a key stored separately from

the database, which helps to keep passwords secure in the event of a database-only compromise.

Single sign-on (SSO)

Customers can also allow team members access by signing into a central identity provider. Our SAML-based SSO implementation streamlines management and improves security by placing a trusted identity provider in charge of authentication, using the same password policies as other services at your organization, and giving team members access to BlueCard without an additional password to manage. BlueCard has also partnered with a leading identity management provider so that users can be provisioned and de-provisioned automatically. Customers are responsible for integrating and managing their identity provider.

Active Directory Integration

Customers are able to automatically provision and de-provision staff accounts by adding and removing users from their existing Active Directory system via our Active Directory connector. Once integrated, Active Directory can be used to manage membership to the BlueCard system.

Encryption

Data at rest

Data at rest in BlueCard's production network is encrypted using industry-standard 256-bit Advanced Encryption Standard (AES256), which applies to all types of data at rest within BlueCard's systems—relational databases, file stores, database backups, etc. All encryption keys are handled by Amazon Web Services (AWS) server-side encryption (SSE) service with no external access allowed to view the keys. BlueCard has implemented appropriate safeguards to protect the creation, storage, retrieval, and

destruction of personal secrets such as SSH keys and service account credentials.

Data in transit

To protect data in transit between our app and our servers, BlueCard supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures, whenever supported by the clients. Additionally, on the web, we flag all appropriate authentication cookies as secure and enable the HTTP Strict Transport Security (HSTS) header. BlueCard uses TLS/SSL exclusively for external connections to make sure that all communications to and from our application are secure. To prevent man-in-the-middle attacks, authentication of BlueCard front-end servers is performed through public certificates held by the client. An encrypted connection is negotiated before the transfer of any data and ensures secure delivery to BlueCard front-end servers.

Key Management

Key management is maintained through AWS' Public Key Infrastructure (PKI) solution, AWS Certificate Manager (ACM) which is designed with operational, technical, and procedural security controls. Access to keys is based on an employee's role as well as having business-impacting need-to-know and the keys themselves are rotated periodically. Encryption key generation, exchange, and storage is distributed for decentralized processing and protected by production system infrastructure security controls and policies.

Internal SSH keys

Access to production systems is restricted with unique SSH key pairs. Security policies and procedures require the protection of SSH keys. An internal system manages the secure public key exchange process, and private keys

are stored securely. Internal SSH keys cannot be used to access production systems unless the account has been specifically added to that environment. Access to the environment is temporary and based on need-to-know.

Key distribution

BlueCard automates the management and distribution of sensitive keys to systems that are required for operations.

Each customer's data is hosted in our shared infrastructure and logically separated from other customers' data. We use a combination of storage technologies to ensure customer data is protected from hardware failures and returns quickly when requested. BlueCard's service is hosted in data centers maintained by industry-leading service providers, offering state-of-the-art physical protection for the servers and infrastructure that comprise the BlueCard operating environment.

Secure Development Lifecycle (SDL)

BlueCard's product security team has built a robust secure development lifecycle, which seeks to make every developer responsible for security by inspiring secure design. We understand that security is a joint effort and should be baked into the entire development process. Thus, we have regular conversations and meetings through Slack and other remote channels to determine strategies for addressing and remediating vulnerabilities. We also understand that in security, user awareness is imperative and so we mandate security training during employee onboarding and periodically throughout the year. Our security team educates developers on secure coding practices, including the use of code libraries that have been vetted for security, and techniques to avoid known coding flaws such as those highlighted in the OWASP Top 10. We do all this and more to ensure that security is part of our

entire development workflow from the conception of a feature to the implementation and maintenance of it.

In addition, BlueCard uses a variety of tools to improve the security posture of everything we build. We perform weekly Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). Risk assessments with remediation/mitigation/avoidance efforts happen semi-annually. Penetration testing is performed by third-party, credentialed cybersecurity auditors at least annually.

Separate development, test, stage, and production environments are used to avoid the risk of introducing security flaws into live systems and minimizing exposure of sensitive data during the development lifecycle.

BlueCard performs strict and frequent application security testing to check against XSS, CSRF, SQL injection, and other vulnerabilities while maintaining that any vulnerabilities found will be addressed and remediated, or mitigated promptly.

Change control processes ensure that new code is tested and approved before being released. Recently modified code is regularly scanned for vulnerabilities.

The security team has automated alerts that are designed to detect the unauthorized activity of a malicious actor, insider, or otherwise, who is attempting to view customer data with no clear business need.

Network Security

BlueCard diligently maintains the security of our back-end network and takes many steps to deny malicious actors' the ability to intercept data.

Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We employ industry-standard protection techniques, including securely-configured firewalls, vulnerability scanning, network security monitoring, intrusion detection systems, Web Application Firewalls (WAFs), role-based access controls (RBACs), access control lists (ACLs), security groups, MFA, and a least privilege access policy to ensure only eligible and non-malicious traffic is able to reach our maintenance protocols, infrastructure, and the networks that host it.

BlueCard configures all ACLs, security groups, ports, protocols, and services to *deny-all by default and permit-by-exception*. This ensures that BlueCard only exposes the appropriate interfaces necessary for our customers to use the service and limits the attack surface. We run scanners and automated tools to verify that these resources are properly protected.

Internal access requires layers of authentication that include strong, complex passwords, SSH keys, 2FA, and one-time passcodes.

Strict limitation is maintained between the internal BlueCard network and the public internet. Internet-bound traffic to and from the production network is carefully controlled through a dedicated proxy service and those, in turn, are protected by restrictive firewall rules. Servers are configured as bastion hosts with each server containing only the services it absolutely needs. No other software is added to the host in order to maintain a limited attack surface. At the single network point of entry, the network intrusion detection & prevention systems are installed, with active monitoring, filtering, and an alerting system. Every connection to our hosts is SSL encrypted using a proven, peer-reviewed, and open-source encryption algorithm to prevent network sniffing, injection, and other attacks.

Access to the production environment is restricted to authorized IP addresses only and requires multi-factor authentication on all endpoints, as well as passing an extensive background check. IP addresses with access are associated with the corporate VPN or approved BlueCard personnel. Authorized IP addresses are reviewed on a quarterly basis to ensure a secure production environment. Access to modify the IP address list is restricted to authorized individuals.

BlueCard uses sophisticated agents to monitor our servers, laptops, and desktops for malicious events, regardless of if they are running Linux, Mac, or Windows operating systems. Security logs are collected in a centralized location for forensic and incident response following the industry-standard retention policy and are also backed up off-site for redundancy.

We use Infrastructure-as-Code (IaC) tools, like CloudFormation, to create all of BlueCards's resources and to ensure that baseline security configurations are consistently pushed out to all servers. Any changes made to the CloudFormation templates are first scanned by Cloudsploit and are required to go through BlueCard's change control processes.

BlueCard strives to have all servers hardened to NIST 800-53 (version 5) level standards where possible.

The BlueCard security team is responsible for maintaining infrastructure security and ensuring that server, firewall, and other security-related configurations are kept up to date with industry standards. Firewall rule sets and individuals with access to production servers are reviewed on a periodic basis.

BlueCard identifies and mitigates risks via regular network security testing and auditing by both a dedicated internal security team and third-party security specialists.

Vulnerability Management

BlueCard has management processes in place to identify, triage, and mitigate vulnerabilities. Our security team performs automated and manual application security testing on a regular basis to identify and patch potential security vulnerabilities and bugs on our application. As part of this effort, we run vulnerability scans pointed at both internal and external endpoints, triage potential vulnerabilities, and work with developers to patch any issues found.

Scanning and penetration testing

BlueCard contracts with third-party vendors to perform periodic penetration and vulnerability tests on the corporate and production environments all to help keep our applications secure. The input from these activities is assessed by our security team, and priorities are assigned to items based on severity. A necessary component of our information security management system is the reporting of findings and recommendations that result from all of these assessment activities to BlueCard management, as well as the evaluation, and appropriate action taken, as determined to be necessary by the security team and BlueCard management. High-severity items are documented, tracked, and resolved by assigned security engineers.

Change management

BlueCard's change management procedures, as defined by BlueCard's engineering and security teams, ensure that application changes have been

properly tested and authorized prior to implementation into the production environments. Source code changes are initiated by developers seeking to make an enhancement to the BlueCard application or service. Changes are stored in our version control system and go through automated and manual quality assurance (QA) testing procedures to verify that security requirements are met. Successful completion of QA procedures leads to the implementation of the change. QA-approved changes are automatically implemented in the production environment through our CI/CD pipeline.

Our software development lifecycle (SDL) requires adherence to secure coding guidelines, as well as the screening of code changes for potential security issues via our automated QA and manual review processes. Changes released into production are logged and archived, and alerts are sent to BlueCard engineering team management automatically. Changes to BlueCard infrastructure are restricted to authorized personnel only.

Protective monitoring

The ability to gather, synthesize, and alert on security-relevant events is fundamental to any cybersecurity risk management program. BlueCard continuously monitors its systems for unauthorized activity that may result in the exposure of sensitive data.

Comprehensive centralized auditing and logging validate privacy and data protection policies and ensure visibility into activity within the platform, including an intrusion detection system to watch for any suspicious or unauthorized activity and assist in a forensic investigation in the event of a compromise. Our security team gets alerts of any critical issues in real-time. Some of the tools we use to achieve near-real-time detection and response for critical events while filtering out false positives and low/accepted risks:

- **AWS CloudTrail**
  Generates logs for all API calls and console events. Logs are digitally signed and encrypted, and are redundantly stored in a secure Amazon S3 bucket.

- **Virtual Private Cloud (VPC) Flow Logs**
  Monitors all network activity going in and out of our VPC.

- **Amazon CloudWatch**
  Monitors our AWS environment and generates alerts similar to a Security Information Event Management (SIEM) system.

- **Vanta**
  Monitors multiple aspects of our attack surface including employee devices (ensuring anti-malware, HDD encryption, etc. are in place), monitoring AWS resources for potential configuration vulnerabilities, and tracking necessary patches/updates.

Each of these logs is reviewed on a bi-weekly basis. This allows the BlueCard security team to identify and address any events that may occur within our systems.

Incident management

BlueCard has pre-planned incident management processes in place to ensure that we can identify and respond to security incidents and events and recover our services. We have established policies and procedures (also known as runbooks) for responding to potential incidents. The runbooks define the types of events that must be managed via the incident response process and classifies them based on severity. We also perform tabletop exercises to identify bottlenecks and shorten our response time in the event

of an incident. In the case of an incident, affected customers will be informed via email from our support team. Incident response procedures are tested and updated on a quarterly basis.

Information Security

BlueCard has established an information security management framework describing the purpose, direction, principles, and basic rules for how we maintain trust. This is accomplished by assessing risks and continually improving the security, confidentiality, integrity, availability, and privacy of our systems.

Our policies

Only the organizations that you want to have access to your data should be able to access it. To that end, we've established a thorough set of security policies that are designed to protect your data and limit the collection, use, and dissemination of your information without your authorization. These policies are reviewed and approved at least annually and are enforced by the BlueCard security team.

Part of keeping our service secure is making sure that people who work at BlueCard understand how to be security-conscious and recognize suspicious activity. To that end, BlueCard has implemented formal, documented security awareness and training policies and procedures for our employees, interns, and contractors that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Our security policies cover:

- **Information security**

  How we limit access to information and information processing systems, networks, and facilities to authorized parties.

- **Operations security**

  How we ensure the correct and secure operation of information processing systems and facilities.

- **Asset management**

  How we protect user data, and the assets storing or processing it against physical tampering, loss, damage, or seizure.

- **Secure development**

  How we design and develop our services to identify and mitigate threats to their security that could compromise your data, cause loss of service or enable other malicious activity.

- **Risk management**

  How we assess and manage BlueCard's information security risks in order that it plays an integral part in the governance and management of the organization at a strategic and operational level.

- **HIPAA compliance**

  How we protect electronic health information so that clients subject to the requirements of HIPAA can use BlueCard to fulfill their regulatory requirements.

- **Incident response**
  How we respond to potential security incidents, including assessment, communication, and investigation procedures.

- **Business continuity**
  How we prepare for events of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

- **Subprocessor management**
  How we ensure that our supply chain satisfactorily supports all of the security principles which the service claims to implement.

We regularly review and update security policies, provide security training, perform application and network security testing (including penetration testing), monitor compliance with security policies on a 24/7 basis, and conduct internal and external risk assessments.

Our employees and contractors

Upon hire, each BlueCard employee, intern, or contractor is required to complete a background check (specific to US citizens), sign a security policy acknowledgment, non-disclosure agreement, and receive privacy, confidentiality, and security training. Only individuals that have completed these procedures are granted access to our internal tools, customer data, corporate, development, and production environments, and then only on an as-needed basis.

Employees and contractors also receive regular security awareness training via informational talks, tabletop exercises, phishing tests, and presentations.

Employee and contractor access to the BlueCard environment is authenticated using a combination of strong passwords, passphrase-protected SSH keys, two-factor authentication, and OTP emailed-tokens. Remote access requires the use of a VPN protected with two-factor authentication, and any special access is reviewed and vetted by the security team. Firewall configurations are tightly controlled and limited to a small number of administrators.

In addition, our internal policies require employees and contractors accessing production and corporate environments to adhere to best practices for the creation and storage of SSH private keys. Access to other resources, including server configuration utilities, production servers, and source code development utilities is granted through explicit approval by appropriate management.

BlueCard employs technical access controls and internal policies to prohibit employees from arbitrarily accessing user data and other information about users' accounts. In order to protect end-user privacy and security, only a small number of engineers responsible for developing core BlueCard services have access to the environment where user data is stored. Employee and contractor access is revoked as soon as possible when an employee leaves the company (always within 24 hours).

Physical Security And Reliability

BlueCard was developed with multiple layers of redundancy to guard against data loss and ensure availability. Incremental backups are performed hourly, and full backups are performed every day. BlueCard tests backups at least quarterly to ensure that they can be successfully restored.

All customer data resides entirely in our AWS production environment, which is a multi-tenant solution where data is logically separated and allows us to benefit from the many advanced reliability solutions that are designed to provide annual data durability of at least 99.99999%. Physical protections are entirely provided by AWS, which has world-class physical and environmental security, including strictly controlled perimeters, ingress points with video surveillance, on-site security, and two-factor authentication, in addition to a wide range of security certifications and attestations as to its physical security. More data on AWS data center security can be found here.

Transparency

BlueCard makes available a third-party site that communicates the status of our service. As a current customer, you can visit status.mybluecard.org at any time to view the current site status, as well as past disruptions and maintenance.

BlueCard will also notify affected clients in the event of a data breach, as required by applicable law and contractual obligation, in the most expedient way possible and without unreasonable delay.

We maintain incident response policies and procedures that are audited as part of our SOC 2 Type II security assessments, including a breach notification process, which enables us to notify affected customers as needed. As part of our incident response procedures, we have a dedicated team that is trained to:

- Promptly respond to alerts of potential incidents
- Determine the severity of the incident
- If necessary, execute mitigation and containment measures
- Communicate with relevant internal/external stakeholders, including notification to affected customers
- Meet breach or incident notification contractual obligations and to comply with relevant laws and regulations
- Gather and preserve evidence for investigative efforts
- Document a postmortem and develop a permanent triage plan

Subprocessors

BlueCard corporate and production systems are housed at third-party managed service providers located in different regions of the United States. These subprocessors (external providers that process customer data) are evaluated by BlueCard's security personnel to ensure that they employ adequate security controls throughout their respective environments. Subprocessors' SOC 2 reports, ISO certifications, and/or vendor security questionnaires, and contractual obligations are reviewed at a minimum annually for sufficient security controls. Subprocessors are responsible for the physical, environmental, and operational security controls at the boundaries of BlueCard infrastructure. BlueCard is responsible for the logical, network,

and application security of our infrastructure housed at third-party data centers.

We do provide contractual commitments through our Terms of Service (ToS) or a Master Services Agreement (MSA) to ensure that third-party providers maintain, at a minimum, reasonable levels of security.

In the event these audits or reviews have material findings, that we determine present risks to BlueCard or our customers, we'll work with the subprocessor to understand any potential impact to customer data and track their remediation efforts until the issue has been resolved.

Our subprocessor for processing and storage, AWS, is responsible for the logical and network security of BlueCard services provided through their infrastructure and for ensuring the removal of data from disks allocated to BlueCard's use before they are repurposed.

Compliance

There are many different compliance standards and regulations. Our approach is to align with most accepted standards—SOC 2, ISO 27001, and more—and offer solutions to help our customers meet their compliance obligations governing the collection and use of data, including those under the Federal Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA).

We use independent third-party auditors to rigorously and routinely test our systems, practices, and controls against some of the most widely accepted security standards and regulations in the country, such as SOC 2 and HIPAA.

These reviews occur at least annually and are conducted by well-respected audit and security firms that are independent and thorough in their inspections.

Penetration testing is performed by third-party, credentialed cybersecurity auditors at least annually.

In addition, we use a 24/7 continuous security monitoring solution to support our compliance risk management objectives and to monitor our internal systems and controls, in order to ensure compliance with required standards and regulations.

SOC

Service Organization Controls (SOC) Reports, known as SOC 1, SOC 2, or SOC 3, are frameworks established by the American Institute of Certified Public Accountants (AICPA) for reporting on internal controls implemented within an organization.

BlueCard has validated its systems, applications, people, and processes through an audit by an independent third-party, Prescient Assurance LLC, an independent CPA and leader in security and compliance certifications for B2B SAAS companies worldwide. Prescient is trusted by many of the most trusted organizations in the world, like Citibank, Deutschebank, PWC, and others, to independently attest to the security of their systems.

SOC 3 for Security, Availability, and Confidentiality

The SOC 3 assurance report covers the Trust Criteria for Security, Availability, and Confidentiality. The BlueCard general-use report is an executive summary of the SOC 2 report and includes the independent third-party auditor's opinion on the effective design and operation of our controls.

View the BlueCard SOC 3 examination.

SOC 2 for Security, Availability, and Confidentiality

The SOC 2 report provides customers with a detailed level of controls-based assurance, covering the Trust Service Criteria for Security, Availability, and Confidentiality. The SOC 2 report includes a detailed description of BlueCard's processes and the more than 100 controls in place to protect your data. In addition to our independent third-party auditor's opinion on the effective design and operation of our controls, the report includes the auditor's test procedures and results for each control over the course of a specified period of monitored time.

The SOC 2 Type II examination for BlueCard is available upon request under a non-disclosure agreement.

HIPAA

BlueCard will sign business associate agreements (BAAs) with customers who require them in order to comply with the Health Insurance Portability and Accountability Act (HIPAA). BlueCard makes available a third-party assurance report evaluating our controls for the HIPAA Security, Privacy, and Breach Notification Rules, as well as a mapping of our internal practices and recommendations for customers who are looking to meet the HIPAA Security and Privacy rule requirements with BlueCard. Since HIPAA does not have a set of controls that can be assessed or a formal accreditation process, covered entities and business associates, like BlueCard, are HIPAA-eligible based on alignment with NIST 800-53 security controls that can be tested and verified in order to place services on the HIPAA eligibility list. The mapping between the NIST Cybersecurity Framework (CSF) and the HIPAA Security Rule promotes an additional layer of security since assessments performed for

certain categories of the NIST CSF may be more specific and detailed than those performed for the corresponding HIPAA Security Rule requirement.

Students and Children (FERPA and COPPA)

BlueCard allows customers to use the services in compliance with the vendor obligations imposed by the US Family Education Rights and Privacy Act (FERPA). Educational institutions with students under the age of 13 can also use BlueCard consistent with the Children's Online Privacy Protection Act (COPPA), provided that they agree to specific contractual provisions requiring the institution to obtain parental consent regarding the use of our services.

Privacy

Our privacy policy is available at mybluecard.org/legal/privacy. The BlueCard Privacy Policy, User Terms, Customer Agreement, and Acceptable Use Policy provide notice of the following terms:

- What kind of data we collect and why
- With whom we may share information
- How we protect this data and how long we retain it
- Where we keep and transmit your data
- What happens if the policy changes or if you have questions

Summary

BlueCard makes it easy to collect, organize, and prioritize safety records while providing the security measures and compliance attestations that child-centric organizations require. To learn more about BlueCard, contact our sales team at sales@mybluecard.org.

Appendix

SOC 2 Controls

BlueCard has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
BlueCard's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
BlueCard's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
BlueCard has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
BlueCard requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
BlueCard's data backup policy documents requirements for backup and recovery of customer data.
BlueCard has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

BlueCard restricts privileged access to the application to authorized users with a business need.
BlueCard restricts privileged access to databases to authorized users with a business need.
BlueCard requires authentication to production datastores to use authorized secure authentication mechanisms, such as a unique SSH key.
BlueCard restricts privileged access to encryption keys to authorized users with a business need.
BlueCard restricts privileged access to the firewall to authorized users with a business need.
BlueCard restricts privileged access to the operating system to authorized users with a business need.
BlueCard restricts privileged access to the production network to authorized users with a business need.
BlueCard ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
BlueCard requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.
BlueCard restricts access to migrate changes to production to authorized personnel.
BlueCard has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

BlueCard's datastores housing sensitive customer data are encrypted at rest.
BlueCard's network is segmented to prevent unauthorized access to customer data.
BlueCard requires passwords for in-scope system components to be configured according to BlueCard's policy.
BlueCard maintains a formal inventory of production system assets.
BlueCard's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.
BlueCard's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
BlueCard requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.
BlueCard conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
BlueCard completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
BlueCard has processes in place for granting, changing, and terminating physical access to company data centers based on authorization from control owners.
BlueCard reviews access to the data centers at least annually.
BlueCard uses firewalls and configures them to prevent unauthorized access.

BlueCard requires visitors to sign in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.
BlueCard has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.
BlueCard purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.
BlueCard uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
BlueCard uses an intrusion detection system to provide continuous monitoring of BlueCard's network and early detection of potential security breaches.
BlueCard reviews its firewall rulesets at least annually. Required changes are tracked to completion.
BlueCard has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
BlueCard's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.
BlueCard encrypts portable and removable media devices when used.

BlueCard has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.
BlueCard deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.
BlueCard's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
BlueCard's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to BlueCard's security incident response policy and procedures.
BlueCard tests its incident response plan at least annually.
BlueCard has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.
BlueCard performs background checks on new employees.
BlueCard requires contractor agreements to include a code of conduct or reference to BlueCard’s code of conduct.
BlueCard communicates system changes to authorized internal users.

BlueCard requires contractors to sign a confidentiality agreement at the time of engagement.
BlueCard requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
BlueCard requires employees to sign a confidentiality agreement during onboarding.
BlueCard managers are required to complete performance evaluations for direct reports at least annually.
BlueCard's board of directors has a documented charter that outlines its oversight responsibilities for internal control.
BlueCard management has established defined roles and responsibilities to oversee the design and implementation of information security controls.
BlueCard maintains an organizational chart that describes the organizational structure and reporting lines.
Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
BlueCard requires employees to complete security awareness training within thirty days of hire and annually thereafter.
BlueCard utilizes a log management tool to identify events that may have a potential impact on BlueCard's ability to achieve its security objectives.

BlueCard performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
BlueCard has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
BlueCard's information security policies and procedures are documented and reviewed at least annually.
BlueCard provides a description of its products and services to internal and external users.
BlueCard has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.
BlueCard's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).
BlueCard notifies customers of critical system changes that may affect their processing.
BlueCard provides guidelines and technical support resources relating to system operations to customers.
BlueCard specifies its objectives to enable the identification and assessment of risk related to the objectives.

BlueCard has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.
BlueCard has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.
BlueCard has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
BlueCard has a documented business continuity/disaster recovery (BC/DR) plan and tests it annually.
BlueCard's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
BlueCard has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - annual review of critical third-party vendors.