Making IT Secure

Security & Risk Management Overview

Last Update: July 2019

Blue Star Security Overview

1 OUR COMPANY AND SYSTEMS

Blue Star in New Zealand is a leading print communications group, organised as a confederation of independent businesses offering New Zealand's leading corporates and companies online services and production solutions. These online services are available to customers as purpose-built and developed portals and web applications with built in RESTful Web Service interfaces.

2 SECURITY AND RISK GOVERNANCE

Blue Star's primary security focus is to safeguard our customers' and users' data. This is the reason that Blue Star has invested in the appropriate resources and controls to protect and service our customers. This investment includes the implementation of the ISMS system and team responsible for the security and risk management program and the governance process. The security team is focused on defining new and refining existing controls, implementing and managing the Blue Star security framework as well as providing a support structure to facilitate effective risk and incident management. Our Group IT Manager, who reports to the Chief Executive Officer, manages the Security Team.

3 SECURITY AND RISK MANAGEMENT OBJECTIVES

We have developed our ISMS system using the ISO 27001 framework. Our key objectives include:

- Customer Trust and Protection – consistently deliver superior product and service to our customers while protecting the privacy and confidentiality of their information.
- Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized individuals and proactively minimize the security risks threatening service continuity
- Information and Service Integrity – ensure that customer information is never corrupted or altered inappropriately.
- Compliance with Standards – implement process and controls to align with current international regulatory and industry best practice guidance. We have designed our security program around best-of-breed guidelines and align our practices with ISO 27001 standards.

4 SECURITY CONTROLS

In order to ensure we both business and client data, we have implemented an array of security controls. Blue Star's security controls are designed to allow for a high level of employee efficiency without artificial roadblocks, while minimizing risk. The following sections describe a subset of controls. For more information about the Blue Star security program, please check out all the details at https://www.bluestar.co.nz/security.

4.1 INFRASTRUCTURE

4.1.1 DATA CENTER SECURITY

Blue Star has outsourced key components of its infrastructure to leading cloud and datacenter infrastructure providers, Blue Star leverages Amazon Web Services (AWS) for DNS, Load Balancing and Portal Proxy services and Spark for Datacenter Internet, Network and Server Co-Hosting services. These solutions provide high levels of physical and network security and well as hosting provider vendor diversity. At present, Blue Star's AWS cloud server instances reside in the Sydney location and co-hosted server hardware at the Popes Road, Takanini location. Both providers maintain an audited vendor security program and ISO 27001 compliance and certification.

These world-class infrastructure providers leverage the most advanced facilities infrastructure such as power, networking, and security. Facilities uptime is guaranteed between 99.95% and 100%, and the facilities ensure a minimum of N+1 redundancy to all power, network, and HVAC services. Access to these providers' sites is highly restricted to both physical access as well as electronic access through public (internet) and private (intranet) networks in order to eliminate any unwanted interruptions in our service to our customers.

The physical, environmental, and infrastructure security protections, including continuity and recovery plans, have been annually reviewed and validated as part of both their ISO 27001 certification and the Blue Star Vendor Management program.

4.1.2 NETWORK SECURITY & PERIMETER PROTECTION

The Blue Star infrastructure is built with internet-scale security protections in mind. In particular, network security protections are designed to prevent unauthorized network access to and within the internal product infrastructure. These security controls include enterprise-grade routing and network access control lists (firewalling) using a Cisco Firewall, Switch, WiFi and Intrusion Protection stack.

Internet Network-level access control lists are implemented in Cisco ASA firewall rules, which applies port- and address-level protection to traffic in the infrastructure and to external networks and users. This allows for finely grained control for network traffic from a public network as well as between server instances on the interior of the infrastructure. Within the infrastructure, internal network restrictions allow a many-tiered approach to ensuring only the appropriate types of devices can communicate. Networks on the WAN are segmented to manage internal subnet access.

User Network access is managed using ISO Accredited Forcepoint Web (AP-WEB) and Mail (AP-MAIL) Security gateway stack of products.

Changes in the network security model are actively monitored and controlled by standard change control approval processes. All existing rules and changes are evaluated for security risk and captured appropriately. Activity and Logs from the network systems are reviewed monthly.

4.1.3 CONFIGURATION MANAGEMENT

Server instances are fully monitored and managed, meaning that any server's configuration is tightly controlled from birth through deprovisioning.

Changes to the configuration are managed through a controlled change management process. Each instance type includes its own hardened configuration, depending on the deployment of the instance.

Patch management and configuration control is managed by Desktop Central which identifies both operating and third-party system patching.

4.1.4 ALERTING & MONITORING

Blue Star invest in automated external service uptime monitoring using 24x7 to ensure uptime and performance of client applications are operating and meet agreed SLA's. Blue Star also use Nagios for monitoring, alerting and response to manage resource utilisation and performance.

The Blue Star infrastructure is designed to detect system issues, uptime issues, application attacks, and other anomalies trigger automatic responses and alerts to the appropriate teams for response, investigation, and correction. As unexpected or malicious activities occur, systems bring in the right people to ensure that the issue is rapidly addressed.

Logs and events are monitored and are escalated immediately to take appropriate action.

4.1.5 INFRASTRUCTURE ACCESS

Access to Blue Star's systems are strictly controlled. Blue Star employees are granted access to corporate services and infrastructure based on their jobs, using a role-based access control model.

For access to infrastructure tools, servers, and similar services, access is minimized to only the individuals whose jobs require it.

Additionally, direct network connections to infrastructure devices is prohibited, and administrators / engineers are required to authenticate first through a Cisco VPN using Cisco DUO two factor authentication before accessing QA or production environments. Server-level authentication uses Cisco DUO two factor authentication also for administrator access.

4.2 APPLICATION PROTECTION

4.2.1 WEB APPLICATION DEFENSES

As part of its commitment to protecting customer data and websites, Blue Star implements online systems aligned to the best practice guidelines documented by the Open Web Application Security Project (OWASP) in the OWASP Top 10 and similar recommendations.

4.2.2 DEVELOPMENT & RELEASE MANAGEMENT

One of Blue Star's greatest advantages is our constantly improving solutions and our approach to software development. New code is developed and controlled using a prescribed Software Development Life Cycle, which includes design scoping, QA testing and approved deployment cycles.

All code deployments create archives of existing production-grade code in case failures are detected by post-deploy hooks. The deploying team manages notifications regarding the health of their applications. If a failure occurs, roll-back is immediately engaged.

4.2.3 VULNERABILITY SCANNING, PENETRATION TESTING, & BUG BOUNTIES

The Blue Star Security team manages a multi-layered approach to vulnerability scanning, using a variety of industry-recognized tools to ensure comprehensive coverage of our technology stack. We perform continuous cloud based vulnerability scanning and penetration testing activities against our client system on a continuous basis using SecOps Tenable IO, using ISO 27001 compliant scan profiles.

Blue Star also engages SecLabs an ISO 27001 certified penetration testing team, who conduct annual active third parties penetration tests annually. The goal of these programs is to iteratively identify flaws that present security risk and rapidly address any issues. Penetration tests are performed against the application layers and network layers of the Blue Star technology stack, and penetration testers are given internal access to the Blue Star product and/or corporate networks in order to maximize the kinds of potential vectors that should be evaluated.

4.3 CUSTOMER DATA PROTECTION

4.3.1 CONFIDENTIAL INFORMATION

The Blue Star ensures only the capture of appropriate information to support the functioning of our online systems. The Blue Star systems are not used to collect or capture sensitive data such as credit or debit card numbers, personal financial account information, Social Security numbers, passport numbers, driver's license numbers or similar identifiers, or employment, financial or health information.

4.3.2 CREDIT CARD INFORMATION PROTECTION

Blue Star customers who pay for any goods or services by credit card. Blue Star are protected as we do not store, process or collect credit card information submitted to us by customers. We leverage Payment Express for PCI-DSS compliant authorization and ensure that customers' credit card information is processed securely and according to appropriate regulations.

4.3.3 ENCRYPTION IN-TRANSIT & AT-REST

All sensitive interactions with the Blue Star products (e.g., API calls, login, authenticated sessions to the customer's portal, etc.) are encrypted in-transit with TLS 1.0, 1.1, 1.2 or 1.3 and 2,048 bit keys or better. Customers who would like to limit the encryption protocols used for HTTPS connections may start the process by contacting Customer Support as an exception to our normal standards.

Blue Star leverages several technologies to ensure stored data is encrypted at rest. These solutions are enabled for "high risk" servers or systems on request. Physical hard-drive encryption and file level encryption are used by Blue Star in these instances using Bit-Locker or PGP encryption. Additionally, certain databases or field-level information is encrypted at rest, based on the sensitivity of the information. For instance, Blue Star Portal user passwords are hashed.

4.3.4 USER AUTHENTICATION & AUTHORIZATION

The Blue Star products enforce a uniform password policy. The password policy requires a minimum of 8 characters that include a combination of lower and upper case letters, special characters, whitespace, and numbers. The minimum requirement cannot be changed on a per-portal basis. Users may also configure two-step verification using email based authorisation to provide second factor when logging in.

Customers can assign finely grained permissions to the users in their portals and limit access to the portal's content and features. For more information about user roles, please see the Blue Star User Roles and Permissions Guide.

Application programming interface (API) access is enabled through Blue Star Portal username and password access. The access is defined at a customer level and limits data access to the client access scope defined.

4.3.5 EMPLOYEE ACCESS

Blue Star controls individual access to data within its production and corporate environment. A subset of Blue Star's employees are granted access to production data based on their role in the company through user access requests authorized by General or Finance Manager level users.

Blue Star's internal network is segregated into three access levels. The BSPGNZ network provides domain access to all assigned resources, BSPGNZ-mobile provides limited mobile access to basic mail and internet services, BSPGNZ-Guest provides outbound internet only access with weekly changing passwords.

Blue Star's highly privileged users are required to use Cisco DUO (two-factor authentication) to access VPN and remote desktop server access.

4.4 PRIVACY

The privacy of our customers' data is one of Blue Star's primary considerations. As described in our Privacy Policy, we never sell your Personal data to any third parties. The protections described in this document and other protections that we have been implemented are designed to ensure that your data stays private and unaltered. The Blue Star products are designed and built with customer needs and privacy considerations in the forefront. Our privacy program incorporates best practices, customers' and their contacts' needs, as well as regulatory requirements.

4.4.1 DATA RETENTION POLICY

Customer data is retained for as long as you remain a customer and until impractical, your data will remain in the Blue Star's system indefinitely. Former customers' core data is removed from live databases upon a customer's written request or after an established period following the termination of all customer agreements. In general, former customers' data is purged 90 days after all customer relationships are terminated. Information stored in replicas, snapshots, and backups is not actively purged but instead naturally ages itself from the repositories as the data lifecycle occurs. Blue Star reserves the right to alter the data pruning period and process at its discretion in order to address technical, compliance, or statutory needs.

4.4.2 PRIVACY PROGRAM MANAGEMENT

Blue Star's Legal, Security, and several other teams collaborate to ensure an effective and consistently implemented privacy program. Information about our commitment to the privacy of your data is described in greater detail in our Privacy Policy.

4.5 BUSINESS CONTINUITY & DISASTER RECOVERY

Blue Star maintains business continuity and disaster recovery plans focusing both on preventing outage through redundancy of telecommunications, systems and business operations, and on rapid recovery strategies in the event of an availability or performance issue. Whenever customer-impacting situations occur, Blue Star's goal is to quickly and transparently isolate and address the issue. Identified issues are published on Blue Star's 24x7 status site and are subsequently updated until the issue is resolved.

4.5.1 SYSTEM RESILIENCY & RECOVERY

Business continuity testing is part of Blue Star normal processing. Blue Star recovery processes are validated annually through its contractual arrangement with its DR partner, Lexel Systems.

Blue Star primarily relies on infrastructure redundancy, real time replication and backups. All Blue Star product services are built with full redundancy. Server infrastructure is strategically distributed across multiple hardware nodes.

4.5.2 BACKUP STRATEGY

Blue Star ensures data is replicated and backed up in multiple durable data-stores. The retention period of backups depends on the nature of the data. In addition, the following policies have been implemented and enforced for data resilience:

- Customer (production) data is backed up leveraging offsite replication for immediate data protection. All production databases have no less than 1 primary (master) and 1 replica (slave) copy of the data live at any given point in time. Seven days worth of backups are kept for any database in a way that ensures restoration can occur easily. Snapshots are taken and stored to a secondary service no less often than daily and where practicable, real time replication is used.
- Because we leverage private cloud services for hosting, backup and recovery, Blue Star does not implement physical infrastructure or physical storage media within its products. Blue Star does also not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.
- By default, all backups will be protected through access control restrictions on Blue Star product infrastructure networks, access control lists on the file systems storing the backup files and/or through database security protections.

4.6 CORPORATE SECURITY

4.6.1 EMPLOYEE AUTHENTICATION & AUTHORIZATION

Blue Star enforces an industry-standard corporate password policy. That policy requires changing passwords at least every 90 days. It also requires a minimum password length of 8 characters and

complexity requirements including special characters, upper and lower case characters, and numbers. Blue Star prohibits account and password sharing by multiple employees.

Employees generally authenticate to Blue Star product infrastructure using remote or local network login. Where passwords are allowed, the password policy requires 8 character passwords. Additionally, critical or high risk assets require multi-factor authentication or are protected by single-signon solutions that are being enabled with multi-factor authentication.

4.6.2 ACCESS MANAGEMENT

Blue Star has regimented and automated authentication and authorization procedures for employee access to Blue Star systems. All access is logged. Most frequently, access is granted based on a role-based access control model.

We have enabled our Helpdesk systems to streamline and automate our security management and compliance activities. In addition we review inactivity and non-use on a monthly basis to revoke accounts and access where needed. These internal systems sweep the infrastructure validating that it meets approved configurations on a 24-hours basis.

4.6.3 BACKGROUND CHECKS

All Blue Star employees undergo an extensive 3rd party background check prior to formal employment offers. In particular, employment, education, and criminal checks are performed for all potential employees. Reference verification is performed at the hiring manager's discretion. All employees receive security training within the first month of employment as part of the Blue Star security program along with role-specific follow-up training. All employees must comply with Non-Disclosure Agreements and Acceptable Use Policy as part of access to corporate and production networks.

4.6.4 VENDOR MANAGEMENT

We leverage a small number of 3rd party service providers who augment the Blue Star solutions. We maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support Blue Star.

Appropriate safeguards are assessed relative to the service being provided and the type of data being exchanged. Ongoing compliance with expected protections is managed as part of our contractual relationship with them. Our Security team and the business unit who owns each contract coordinate unique considerations for our providers as part of contract management.

4.6.5 SECURITY AWARENESS & SECURITY POLICIES

To help keep all our administrators, support, and other employees on the same page with regard to protecting your data, Blue Star developed and maintains a Written Information Security Policy. The policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics.

With this policy and the myriad protections and standards in place, we also ensure Blue Start staff are well-trained for their roles. Multiple levels of security training are provided to Blue Star employees,

based on their roles and resulting access. General security awareness training is offered to all new employees and covers Blue Star security requirements.

4.7 Incident Management

Blue Star provides 24x7x365 coverage to respond quickly to all security and privacy events. Blue Star's rapid incident response program is responsive and repeatable. Pre-defined incident types, based on historical trending, are created in order to facilitate timely incident tracking, consistent task assignment, escalation, and communication. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others.

In responding to any incident, we first determine the exposure of the information and determine the source of the security problem, if possible. We communicate back to management (and any other affected customers) via email or phone (if email is not sufficient). We provide periodic updates as needed to ensure appropriate resolution of the incident.

Our Group IT Manager reviews all security-related incidents, either suspected or proven, and we coordinate with affected businesses and management using the most appropriate means, depending on the nature of the incident.

5 PRODUCT SECURITY FEATURES

Blue Star's security program is designed to protect all of the Blue Star systems. Each product takes advantage of common application development security best practices as well as infrastructure security and high availability configurations.

Blue Star works hard to maintain the privacy of data you entrust with us. Customer Data stored in Blue Star's systems remain the property of its clients. We put our security program in place to protect it, and use it only to provide the Blue Star services. We never share your data across customers and never sell it.

5.1 BLUE STAR PORTAL

About: The Blue Star Portal is our industry-leading client online solution. It provides easy-to-use and effective tools to manage client online services.

DNS / Proxy: Customer sites hosted on the Blue Star products leverage the protection of AWS load-balancing and Proxy services. When security events occur, Blue Star's Security Operations and Technical Operations teams take immediate action to ensure that your sites are protected continuously 24x7x365.

Co-Hosting: Primary Portal / SSO, Online Applications and Content Management System (DCM) infrastructure is co-hosted in Spark Datacenters. Blue Star's hosting strategy enables additional redundancy capabilities, architecture flexibility, and infrastructure responsiveness. Our deployment processes leverage network security, server security, and availability features, described above.

Transport Layer Security: Blue Star Online systems are by default configured to use TLS certificates use Subject Alternative Names which are managed by our certification authority, DigiCert.

Encryption Options: By default, customer websites using HTTPS are configured to allow TLS 1.0, 1.1, 1.2 and 1.3. We constantly review and update these encryption methods as they become unsecure and retired from a PCI-DSS / ISO 27001 compliance perspective.

Privacy: Blue Star always maintains the privacy of data you entrust with us. Data you store in Blue Star systems is yours. We use it only to provide the Blue Star service to you.

Access control: The Blue Star Portal provides easy to manage and intuitive roles that give the right access for users. This allows for user registration, activation, management and de-activation.

6 THIRD PARTY AUDITS AND CERTIFICATIONS

Blue Star supports the need for Third Party Audits and conducts many such audits on an annual basis. A key factor in the selection of vendors is the compliance or certification to ISO 27001 standards. Blue Star's security roadmap includes and ongoing commitment to evolving our security programmes and the achievement of ISO 27001 certification scoped to support the "Management of Sensitive and Classified Client Data". Blue has engaged the services of BSI Group to provide auditing services to achieve this goal.

7 DOCUMENT SCOPE AND USE

Blue Star values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document (including any related communications) are not intended to create a binding or contractual obligation between Blue Star and any parties, or to amend, alter or revise any existing agreements between the parties.