BLUE STAR
HEALTH & SAFETY POLICY

PURPOSE

The management of Blue Star NZ and all its associated sites are committed to providing and maintaining a healthy and safe working environment for all employees, contractors, visitors, and any person working on any of Blue Star NZ premises. To achieve this, we have developed and maintain a system to manage health and safety

MANAGEMENT COMMITMENT

We will

- Set health and safety objectives.
- Annually review health and safety objectives and performance.
- Encourage the accurate and timely reporting and recording of all near misses, incidents and injuries including the early reporting of any pain or discomfort via the Blue Star online H&S system.
- Investigate all reported near misses, incidents, and injuries to ensure all contributing factors are identified and, where appropriate, plans are formulated to take corrective action.
- Provide a treatment and rehabilitation plan that ensures a safe, early, and durable return to work.
- Provide annual health and wellbeing checks to employees and support to employees through EAP counselling services when in need.
- Identify all existing and new hazards, and take what is reasonably practicable to eliminate, or minimise the exposure to any hazards particularly the hazards deemed to be significant.
- Ensure that all workers are made aware of the risks in their work area and adequately trained to enable them to perform their duties in a safe manner.
- Encourage worker consultation and participation in all matters relating to health and safety.
- Promote a system of continuous improvement, including the review of all policies and procedures

LEGISLATIVE COMPLIANCE

Blue Star will meet all obligations under the Health and Safety at Work Act 2015 and the Health and Safety in Employment Regulations 1995, Codes of Practice and any relevant Standards or Guidelines.

EMPLOYEE RESPONSIBILITY

- Every Blue Star employee is expected to share in the commitment to health and safety and play a vital and responsible role in maintaining a safe and healthy workplace by:
- Observing all safe work procedures, rules, and instructions.
- The early reporting of any pain or discomfort.
- Taking an active role in the company's treatment and rehabilitation plan, to ensure an "early and durable return to work"
- Ensuring that all near misses, incidents, injuries, and hazards are reported to the appropriate person in an accurate and timely manner.
- Provide an environment that promotes and empowers feedback from all individuals in relation to Diversity and Inclusion, in respect to ideas, challenges and solutions
- Develop a dashboard of Key Performance Indicators to measure our implementation and continuing success of Diversity and Inclusion.

HEALTH & SAFETY REPRESENTITIVES

The Health and Safety Representatives will actively participate in the implementation, monitoring, review and planning of health and safety polices, systems and safe work practices within Blue Star.

CONTRACTORS & VISITORS

Contractors and Visitors will be briefed on the health and safety requirements of the company in accordance with the Health and Safety at Work Act 2015.

Jill Cowling
Group Chief Executive Officer
Blue Star and Webstar
Effective from January 2020

Reviewed November 2022

BLUE STAR
ENVIRONMENTAL POLICY

As one of the largest marketing execution partners for Kiwi businesses - our group brings together experienced industry leaders in print manufacturing, packaging, print management, design, marketing communications, digital, merchandise and logistics. With manufacturing sites located throughout New Zealand, we are aware of our social and environmental obligations to the local community.

We recognise and understand the environmental impact of our operations.

We have taken pride in environmental stewardship for more than 15 years, and we're dedicated to making improvements in every aspect of quality, health & safety, diversity, well-being, and the environment.

We are committed to operating our company in compliance with all applicable New Zealand laws, rules, and regulations, as well a holding ourselves to high standard in relation to our social, ethical, and business obligations.

Our focus is on

- Reducing (GHG) emissions through reductions of waste to landfill, transport, renewable or sustainably responsible sources without compromising the final product.
- Promotion to our customers to use environmentally sustainable products for end-of-life cycle.

Blue Star is committed to continuously improving our management systems and reviewing our supply chain to ensure we are sourcing from renewable and sustainably responsible sources. All key suppliers are ISO14001 certified.

We consistently review the latest industry technology and software that can lead to reducing (GHG) emissions in consumable waste, energy, and chemical use. Demonstrated in 2018, we introduced new efficient technology to replace 40% of our fleet of traditional offset presses, representing our commitment through investment to our environmental practice.

We use biodegradable (mineral-free) vegetable inks that have a low environmental impact because they are made primarily from renewable resources (soybean/ linseed and pine resin).

Blue Star significantly altered its substrate procurement strategy in 2006, severing ties with several unsustainable overseas mills and challenging our supply chain to do the same. A significant amount of our paper meets the chain of custody requirements at every step in the supply chain, from sourcing to distribution, by ensuring that it is sourced from certified forests; FSC (Forest Stewardship Council) and PEFC (Programme for the Endorsement of Forest Certification). We actively promote sourcing our packaging boards from our local mill in Whakatane to further reduce emissions and support local businesses.

We have partnered with Toitu Enviromark, achieving their Gold Standard in 2021 in all our plants Nationwide, joined the Toitu Carbon Reduce programme in 2022, and we hold a HACCP food safety certification in our Wellington plant since 2021. These programmes supply guidance and verification of our commitment to be doing what we say we are doing, year-on-year reductions and tracked projects yielding improvements. They hold us to account with annual external audits ensuring we are striving to meet the goals and targets we set.

Blue Star maintains a 'Diversity and Inclusion' policy that supports and empowers our 500+ employees. Our ethos and people are our key differentiators and greatest assets. Our Blue Skies programme, which includes investing in and training our people, developing skills, adding qualifications, and sourcing talented graduates and apprentices, is a critical component of our ongoing commitment to our people and resources.

Blue Star won both trainer of the year and apprentice of the year at our Industry Awards in 2022, with four finalists from Blue Star businesses. In addition, we have a community involvement programme with a simple goal: to give back to the communities where we live and work by supporting local sports teams, charities, schools, and community organisations. We have a long history of supporting non-profit and community organisations, such as the Paralympics, Variety - the children's charity, the Child Cancer Foundation, Sport Hawkes Bay, and the Christchurch City Mission.

Blue Star seeks and nurtures partnerships that will have a positive impact on the environment and our society, with the common goal of improving the planet for future generations. The bar is set high for excellence in HSE; Health, safety, and the environment are constantly rising, fostered by our people, our focus as an organisation and the services we provide is on continuous improvement daily. We welcome feedback on how we can continue to grow to better meet the needs of our customers.

For further information or supporting documents, please contact your Account Manager.

Jill Cowling
Group Chief Executive Officer
Blue Star and Webstar

Effective from January 2020

Reviewed November 2022

BLUE STAR
DIVERSITY AND INCLUSION POLICY

PURPOSE

Blue Star Group (New Zealand) Limited engages a workforce made up of many individuals with diverse skills, values, backgrounds, and experiences. Blue Star respects and values these people and the benefit their diversity brings to our businesses. They are our key resource, they are doers and ensure we are driving engagement with our customers, delivering innovation, and connecting with our equally diverse customers to deliver better outcomes. We embrace the diversity of our people and what their individuality brings to our workplace.

"Diversity" refers to the characteristics that make us similar to, or different from one another. At Blue Star, diversity encompasses gender, race, religion, ethnicity, age, sexual orientation, disability, physical capability, political opinion, family responsibilities, marital status, education, employment status, cultural background and more. Diversity encompasses a broad spread of experience, culture perspective and lifestyle of those who live in New Zealand and wherever Blue Star does business.

"Inclusion" at Blue Star is about embracing diversity and creating an environment where everyone can thrive and succeed. We understand that diverse backgrounds, experiences, and views lead to an improved workplace for our people, increase engagement and help to strengthen our teams, deliver innovation and performance, ultimately contributing to better relationships with customers and key stakeholders.

POLICY

Blue Star is committed to:

- encouraging people to be themselves and bring out the best of who they are at work, benefiting from individuals thinking, skills and experience.
- employing a diverse range of people who are also representative of our customers, stakeholders and market place.
- celebrating and leveraging our differences, to ensure as a business we can be the best we can be.
- ensure that we have policies and processes in place that recognise and support diversity and meet the needs of all our people.
- developing a culture of inclusiveness as a core capability, especially for our leaders.
- demonstrating zero tolerance for any form of discriminatory behaviours
- always demonstrating respect to our customers, stakeholders, shareholders, and supply partners inclusively, while understanding their diversity.

RESPONSIBILITY FOR POLICY

Although the board retains ultimate accountability for this policy, the board has delegated responsibility for the implementation of the policy to the Chief Executive Officer.

In turn, the Chief Executive Office has delegated to the HR Manager the administration of this policy, including its reporting.

MEASURABLE OBJECTIVES

Blue Star will have measurable objectives in relation to diversity and inclusion. These will include:

- Ensuring that Diversity and Inclusion is a fundamental consideration for all policies and practices within Blue Star.
- Ensure that all of our people policies and practices are inclusive and consistently executed by all of our leaders.
- Provide an environment that promotes and empowers feedback from all individuals in relation to Diversity and Inclusion, in respect to ideas, challenges and solutions
- Develop a dashboard of Key Performance Indicators to measure our implementation and continuing success of Diversity and Inclusion.

GENERAL

Training may be required for the management to support the successful implementation of

diversity and inclusion initiatives and the achievement of Blue Star's objectives.

Blue Star is committed to supporting diversity and will ensure that we employ or promote the right person for the role based on assessing the specific skills necessary to deliver the position's key accountabilities The 'right person' may have diverse attributes that strongly align with Blue Star's future direction, as opposed to relying on past employment experience to forecast success.

Nothing in this policy will be taken or construed to endorse:

- any discriminatory behaviour by or within Blue Star contrary to the law.
- that the selection and promotion of people at Blue Star being anything other than their ability of adding value to Blue Star and improving the success of Blue Star's short, medium, and long-term objectives.

Jill Cowling
Group Chief Executive Officer
Blue Star and Webstar

Effective from January 2020

Reviewed November 2022

BLUE STAR
QUALITY POLICY

At Blue Star New Zealand, we are committed to delivering the highest quality printed products and services to our customers. Our aim is to consistently meet and exceed customer expectations while adhering to industry standards and best practices. We believe that quality is not just a goal, but a fundamental aspect of our business operations.

Our quality policy is built upon the following principles:

1. **Customer Focus:** We prioritise understanding our customers' needs and requirements to ensure we deliver products that fully meet their expectations. We strive to provide exceptional customer service, effective communication, and timely delivery, while maintaining a customer-centric approach.
2. **Continuous Improvement:** We are dedicated to continuously improving our processes, technologies, and skills to enhance the quality of our products and services. We promote a culture of learning, innovation, and openness to new ideas, which allows us to adapt to evolving customer needs and stay ahead in the print industry.
3. **Compliance with Standards:** We are committed to complying with all relevant legal, regulatory, and industry standards. Our quality management system is designed to ensure that our processes align with recognized quality standards, such as ISO 9001, and that we consistently meet or exceed these requirements.
4. **Employee Empowerment:** We recognise that our employees are our most valuable asset. We provide them with the necessary training, resources, and support to perform their jobs effectively and contribute to the overall quality of our products and services. We encourage employee involvement in quality improvement initiatives and foster a culture of accountability and responsibility.
5. **Supplier Partnerships:** We believe in building strong relationships with our suppliers, treating them as partners in achieving our quality objectives. We select suppliers based on their ability to meet our quality and environmental standards, and we collaborate closely with them to ensure that the materials and services they provide meet our requirements.
6. **Data-driven Decision Making:** We rely on data and metrics to make informed decisions, monitor performance, and drive continuous improvement. We regularly assess our quality performance through audits, inspections, and customer feedback to identify areas for improvement and take appropriate corrective actions.

This quality policy is communicated and understood by all employees within our group of print companies. We regularly review and update our quality objectives to ensure they remain relevant and aligned with our overall business strategy. By adhering to this policy, we aim to provide our customers with print products and services that meet the highest standards of quality, reliability, and customer satisfaction.

For further information, please contact your Account Manager.

Jill Cowling, **Chief Executive Officer**
Blue Star Group (New Zealand) Limited

Effective from January 2020
Reviewed September 2023

BLUE STAR
FOOD SAFETY POLICY

At Blue Star NZ, we are committed to providing safe and high-quality print packaging solutions to our customers. Our aim is to consistently meet and exceed customer expectations while adhering to industry standards and best practices. We believe that quality is not just a goal, but a fundamental aspect of our business operations.

We recognise the importance of food safety in the packaging industry and strive to maintain the highest standards in our operations. This food safety policy outlines our commitment to ensuring the safety of the packaging products we produce.

1. **Compliance with Regulations:** We will comply with all applicable food safety regulations, standards, and legal requirements set forth by local, national, and international authorities. Our operations adhere to guidelines such as Good Manufacturing Practices (GMP), Hazard Analysis and Critical Control Points (HACCP).
2. **Risk Assessment and Management:** We will conduct regular risk assessments to identify potential hazards that may affect the safety of our packaging processes and products. Our risk management approach will involve implementing appropriate control measures to mitigate these risks, ensuring the safety of the products that come into contact with our packaging.
3. **Supplier Approval and Control:** We will establish a formal supplier approval process to ensure that all raw materials used in the production of our packaging materials meet the necessary food safety standards. We will maintain strong relationships with our suppliers, conducting regular audits and assessments to verify their compliance with our food safety requirements.
4. **Training and Awareness:** We will provide training and awareness programs to all employees involved in the production, handling, and quality control of our packaging materials. These training programs will focus on food safety principles, hygiene practices, and the importance of following established procedures to prevent contamination.
5. **Hygiene and Sanitation:** We will maintain a clean and hygienic production environment by implementing robust sanitation procedures. This will include regular cleaning schedules, proper waste management, and the use of appropriate cleaning agents and sanitisers. Personal hygiene practices, such as handwashing and the use of protective clothing, will also be emphasized to ensure the prevention of cross-contamination.
6. **Traceability and Recall Procedures:** We will maintain a robust traceability system that allows us to track the origin and flow of our packaging materials throughout the supply chain. In the event of a quality or safety issue, we will have procedures in place for prompt and effective product recall, ensuring the protection of our customers and consumers.
7. **Continuous Improvement:** We are committed to continuous improvement in our food safety practices. We will regularly review and update our policies and procedures to integrate the latest industry standards and best practices. Feedback from customers, regulatory authorities, and employees will be valued and utilised to drive ongoing improvements.

This food safety policy will be communicated to all employees, suppliers, and stakeholders to ensure their understanding and commitment. Compliance with this policy is mandatory for all individuals associated with Blue Star NZ. We will regularly monitor and review our food safety performance to ensure the effectiveness of our policy and its implementation.

Jill Cowling, **Chief Executive Officer**
Blue Star Group (New Zealand) Limited

Effective from January 2020
Reviewed September 2023

BLUE STAR
MODERN SLAVERY AND HUMAN TRAFFICKING POLICY

PURPOSE

Blue Star Group (New Zealand) Limited engages a workforce made up of many individuals with diverse skills, values, backgrounds and experiences. Blue Star recognises that people are our key resource, they are doers and we, at Blue Star, have policies and processes in place to ensure that slavery or human trafficking is not taking place in any part of our business or our supply chain.

COVERAGE

Blue Star Group (New Zealand) Limited has a number of trading divisions throughout New Zealand which are covered by this policy and statement. These include the following business units: -

- Blue Star Collard (Auckland)
- Blue Star Constellation (Auckland
- Blue Star Swanson (Auckland)
- Blue Star Parnell (Auckland)
- Brebner Print (Napier)
- Blue Star Jackson (Wellington)
- Blue Star Promote (Auckland and Wellington)
- Blue Star Gracefield (Wellington)
- Spectrum Print (Christchurch)

MEANING OF SLAVERY AND HUMAN TRAFFICKING

We recognise that slavery and human trafficking can occur in many forms, such as forced labour, child labour, domestic servitude, sex trafficking and workplace abuse and it can include the restriction of a person's freedom of movement whether that be physical, or non- physical.

OUR SUPPLY CHAINS

Given the diverse nature of our business, we have third party product suppliers and service providers throughout the world who supply goods and services to the Group for the various different business units listed above. Many of our suppliers vary in both the size of their organisations and the amount that we spend with them. Our most significant and material purchase is paper, which we effectively convert during the printing process. All paper that Blue Star business units converts, is imported into New Zealand market.

Blue Star has a mature and robust supply chain and its supply partners have all been vetted over a number of years. Blue Star operates a centralised procurement function and all material sourcing is controlled through Head Office.

In all instances, material contracts are implemented, managed and reported upon at Head Office by the Procurement Manager. Centralised management of the supply chain greatly enhances the vetting process of our suppliers, and has also enabled the organisation to conduct site audits of overseas production facilities.

RISK ASSESSMENT

The risk of slavery and human trafficking within our own organisation is substantially avoided and mitigated as a result of strict policies and procedures, the New Zealand market place, as well as the management structure built into our business operations and the knowledge and skills of our employees.

In relation to the risk of slavery and human trafficking within any of our supply chains, we continuously review the supplier network to consider how to:

- Identify and prioritise potential risk areas across our supply chains, such assessment based upon geography, the product or service we are being provided with and the nature of the business transaction.
- Incorporate this issue into our existing compliance risk assessments, which are carried out annually;
- Mitigate the risk of slavery and human trafficking occurring in the high risk areas identified, more specifically by:
  - Evaluating whether to issue questionnaires to high risk suppliers and service providers requesting information regarding due diligence procedures within their own supply chains;
  - Implementing action plans based on such responses, which seek to work with suppliers to resolve areas of risk and/or modify our supply relationships in order to mitigate or remove risks; and
  - Conducting site visits, where appropriate.

RESPONSIBILITY FOR OUR POLICY

Although the board retains ultimate accountability for this policy, the board has delegated responsibility for the implementation of the policy to the Chief Executive Officer. In turn, the Chief Executive Office has delegated to the HR Manager the administration of this policy, including its reporting.

Jill Cowling
Group Chief Executive Officer
Blue Star and Webstar

Effective from January 2020

Reviewed November 2022

Making IT Secure

Security & Risk Management Overview

Last Update: July 2022

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 and network security monitoring (NDR) using Darktrace.

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 and detection is managed using ISO Accredited Trend Micro system including Mail, Web, Mobile, Apex One and the Vision One 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. All critical changes to firewall access are also automated using Manage Engine newtwork change management (NCM).

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 Manage Engine endpoint central which identifies both operating and third-party system patching.

4.1.4 ALERTING & MONITORING

Blue Star invest in automated external uptime monitoring using 24x7 to ensure uptime and performance of client applications are operating and meet agreed SLA's. Blue Star also use Darktrace for security monitoring, alerting and response to provide EDR / NDR security response.

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 1.2 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 customerimpacting 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 singlesignon 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 NonDisclosure 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 with our security operations partner SecOps, 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 loadbalancing 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.