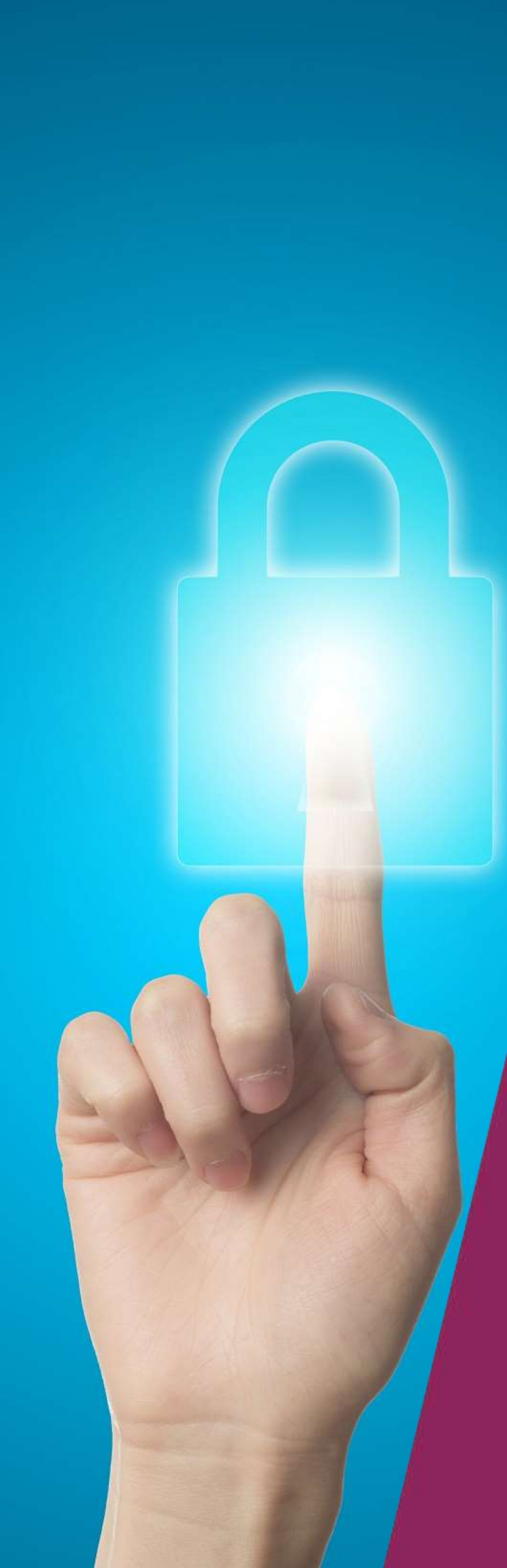

PARABLU

Information Security Management Policy

Parablu Inc.

Table of Contents

Document Control

1. Document Information

Source File Location	**Information Security Folder**
Document Owner	**Suresh Rajendran**
Confidentiality Level	**All Employees**
Proposing Changes	**Write to** itsupport@parablu.com

2. Version History

Version	Date	Author / Editor	Comments
1	**March 31, 2020**	**Suresh Rajendran**	**Initial Draft**
2	**April 8, 2020**	**Anand Prahlad**	**Edits & Finalization**

3	June 15, 2021	Suresh Rajendran	Additions for Incident Management, Thirt Party Risk, BCP & DR, Patch management etc.
4	June 18, 2021	Nagaraj J	Added for Human Resources
5	July 11, 2021	Suresh Rajendran	Additions for Communications and Operation Management Policy
6	July 11, 2021	Anand Prahlad	Edits & Finalization
7	July 12, 2021	Bishal Rai	Formatting
8	August 21, 2021	Anand Prahlad	Refinements to Employee and Visitor ID policy, periodic background checks, software licensing, vendor management etc.

3. Document Reviews and Approvals, Next Review Date

Version	Date	Reviewer / Approver	Comments

Corporate ISMS Policy

4. Purpose

The purpose of the Information Security Management System (ISMS) in Parablu Inc. is to ensure the continuity and protection of business processes and information assets. The information security needs and objectives stated in this document are intended to minimize the impact of security incidents on the operations of Parablu Inc. and its customers.

5. Scope

The primary audiences for Corporate Information Security Policy are: Senior Management, System and Information Owners, Business and Functional Managers, the Chief Information Security Officer (CISO), and IT Security Practitioners of the organization.

6. Definition

- Availability – Property of being accessible and usable upon demand by an authorized entity.
- Asset – Anything that has value to the organization.
- Confidentiality – Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity – Property of accuracy and completeness.
- ISMS – Information Security Management System is part of the overall management system required to establish, implement, maintain, and continually improve information security of the organization.

7. Corporate ISMS Policy

The Information Security Management System of Parablu Inc. intends to ensure:

- Integrity of all business processes, information assets, and supporting IT assets and processes through protection from unauthorized modification, guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The unauthorized modification or destruction of information could have severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- Availability of all business processes, information assets, and supporting IT assets and processes to authorized users when needed, ensuring timely and reliable access to and use of information. The disruption of access to, or use of, information or an information system could have serious adverse effect on organizational operations, organizational assets, or individuals.
- Confidentiality of all information assets (information is not to be disclosed to unauthorized persons through deliberate or careless action). Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The unauthorized disclosure of information could have limited adverse effect on organizational operations, organizational assets, or individuals.
- All IT-enabled processes and stakeholders shall follow the rules and regulations, or circulars published in the organization.
- All audit trails and logs, as decided by the Information Security Team, shall be maintained, and monitored by Parablu Inc.
- All operational and system changes shall be monitored closely; these shall adhere to the change management process.

- Parablu Inc. complies with the laws, regulations and contractual obligations which are applicable to the organization in general and to its ISMS.
- All applicable information security requirements are satisfied.
- Continual improvement of the information security management system.

8. Applicability

This policy applies to all Manager and staff of Parablu Inc., contractors, and third-party employees under contract, who have any access to, or involvement with, the business processes, information assets, and supporting IT assets and processes covered under the scope of ISMS.

9. Responsibility

Parablu Inc. shall ensure that all activities required to implement, maintain, and review this policy are performed. All personnel, regarded as included in the ISMS scope, must comply with this policy statement and its related security responsibilities defined in the information security policies and procedures that support the corporate information security policy. All personnel, even if not included in the ISMS scope, have a responsibility for reporting security incidents and identified weaknesses, and to contribute to the protection of business processes, information assets, and resources of Parablu Inc.

10. Policy Compliance

10.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

10.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

10.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Additionally, the company may at its discretion seek legal remedies for damages incurred because of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

11. Periodic Reviews

11.1 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

11.2 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

12. Ownership and Revision

This policy statement is owned by the Board of Directors of Parablu Inc.. This policy shall be revised at least once in two years by the CISO and at any time that the Board of Directors, or the Information Security Team, decides to do so.

Clean Desk Policy

1. Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

2. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers, and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

3. Scope

This policy applies to all Parablu Inc. employees and affiliates.

4. Policy

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the workday.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Internet Usage Policy

1. Overview

Internet connectivity presents the company with risks that must be addressed to safeguard the facility's vital information assets. These risks include:

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Access to the Internet will be provided to users to support business activities and is to be used only on an as-needed basis to perform their jobs and professional roles.

2. Purpose

The purpose of this policy is to define the appropriate uses of the Internet by Parablu Inc. employees and affiliates.

3. Scope

The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy and are also required to use their common sense and exercise their good judgment while using Internet services.

3.1 Internet Services Allowed

Internet access is to be used for business purposes only**.** Capabilities for the following standard Internet services will be provided to users as needed:

- E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).
- Navigation – Internet access services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool.
- Secure File Transfer -- Using Parablu's BluSync ™ to send data/files and receive in-bound data/files, as necessary for business purposes.
- Video and Phone conferencing facilities – Tools such as Microsoft Teams, Zoom, GoToMeeting, WebEx are authorized for us strictly for business meetings.
- Putty/SSH -- Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the company.
- Remote debugging tools – Company provided licenses of WebEx, TeamViewer, and AnyDesk may be used for the express purpose of debugging product issues at remote customer locations.

Management reserves the right to add or delete services as business needs change or conditions warrant.

All other services will be considered unauthorized access to/from the Internet and will not be allowed.

3.2 Request & Approval Procedures

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

3.2.1 Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy The user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.
Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

3.2.2 Approval

Internet access is requested by the user or user's manager submitting an ***IT Access Request*** form to the IT department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

3.2.3 Removal of privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of a non-employee, or any disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

4. Policy

4.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days.

User Internet access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes.
- IT technical support downloading software upgrades and patches.
- Review of possible vendor web sites for product information.
- Reference regulatory or technical information.
- Troubleshooting
- Business related audio and video conferencing
- Work related training
- Research that is intended to aid the employee in fulfilling their job responsibilities

4.3 Personal Usage

Using company computer resources to access the Internet for personal purposes, beyond a reasonable amount of time during any given day, or for non-emergency purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

4.4 Prohibited Usage

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Using customer information for any purposes outside of the need to provide Parablu's services to that customer
- Using customer information for any technical purposes such as testing or product development – unless explicit permission has been obtained from the customer.
- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.

Unless specifically authorized under the provisions of section 4.3, the following activities are also strictly prohibited:

- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.
- Any ordering (shopping) of items or services on the Internet
- Playing of any games
- Forwarding of chain letters
- Participation in any on-line contest or promotion
- Acceptance of promotional gifts

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation and may ban the downloading of particular file types.

4.5 Software License

The company strongly supports strict adherence to software vendors' license agreements. Any open-source tools if used, should be first reviewed by the InfoSec team to confirm licensablity and possible liabilities for inappropriate usage.

When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications, and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk.

4.6 Expectations of Privacy

4.6.1 Monitoring

Users should consider their Internet activities as constantly monitored and limit their activities accordingly.

Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

4.6.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be

aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

4.7 Maintaining Corporate Image

4.7.1 Representation

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

4.7.2 Company Materials

Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee's manager and the public relations department and will be placed by an authorized individual.

4.7.3 Creating Web Sites

All individuals and/or business units wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained through the IT Department. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the Corporate Communications Directors for initial approval to continue. All company pages are owned by, and are the ultimate responsibility of, the Sr Manager, Marketing.

All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the IT department.

Email Policy

1. Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic communications.

2. Purpose

The purpose of this email policy is to ensure the proper use of Parablu Inc.'s email system and make users aware of what Parablu Inc. deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Parablu Inc. network.

3. Scope

This policy covers appropriate use of any email sent from a Parablu Inc. email address and applies to all employees, vendors, and agents operating on behalf of Parablu Inc..

4. Policy

- All use of email must be consistent with Parablu Inc. policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Parablu Inc. email account should be used primarily for Parablu Inc. business-related purposes; personal communication is permitted on a limited basis, but non-Parablu Inc. related commercial uses are prohibited.
- All Parablu Inc. data contained within an email message, or an attachment must be secured according to the Data Protection Standard.
- All email is considered a Parablu Inc. business record and shall be retained according to Parablu Inc. Record Retention Schedule.
- Parablu Inc. email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Parablu Inc. employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding Parablu Inc. email to a third-party email system (noted in points below). Individual messages which are forwarded by the user must not contain Parablu Inc. confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Parablu Inc. business, to create or memorialize any binding transactions, or to store or retain email on behalf of Parablu Inc.. Such communications and transactions should be conducted through proper channels using Parablu Inc.-approved documentation.
- Using a reasonable amount of Parablu Inc. resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Parablu Inc. email account is prohibited.
- Parablu Inc. employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- Parablu Inc. is not obliged to monitor email messages, but may exercise its right to do so without prior notice.

Anti-Malware Policy

Recommended processes to prevent virus problems:

- Always run the corporate standard, supported anti-virus software on all user endpoints. Windows Defender, if not already installed and active, can be downloaded from a secure Microsoft site, installed, and activated. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash. Flag in Outlook or Office 365 mail reader as "Unacceptable content".
- Delete spam, chain, and other junk email without forwarding, in line with Parablu Inc.'s *Acceptable Use Policy*. Flag in Outlook or Office 365 email as spam or junk.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a hard disk, USB pen drive from an unknown source for viruses before using it.
- Your endpoints are backed up by Parablu's BluVault on a regular basis. Please review the weekly email summary you get regarding your backups and check that backups are

happening regularly and on schedule. If not, please report the matter right away to the IT Department.

- This is by approved exception only - If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, re-enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Keep Auto Update of signatures and On Access / Write Scan functionality along with a daily scan always turned on.
- Run Anti-malware programs which are automatically kept up to date on all development, test, build and release systems.
- Prior to release of a build to deployment, it must be scanned by Kaspersky (another industry recognized Anti-malware solution) besides Windows Defender. This is to ensure that there is no known malicious element or vulnerability within release packages – which in turn may expose customer environments to harm.

Password Protection Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to Parablu Inc.'s and its customer systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Parablu Inc. or company's customer deployed facilities, has access to the company's or customer's network, or stores any non-public company's or its customers' information.

4. Policy

4.1 Password Creation

- All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
- Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

4.2 Password Change

- Passwords should be changed only when there is reason to believe a password has been compromised.
- Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

- Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Parablu Inc information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
- Passwords must not be shared in email messages, or other forms of electronic communication, nor revealed over the phone to anyone.
- If Passwords are to be stored, they should be stored in encrypted files which require a complex password to access. Passwords should never be written and left readable on a whiteboard, or on sticky notes.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Multi-Factor Authentication

Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

4.6 Brute force password attack protection

Although brute force password attacks can be mitigated by using complex passwords, a brute force password attack protection such as reCAPTCHA is highly recommended to thwart such attacks.

4.7 Related Standards, Policies and Processes

Password Construction Guidelines

Password Construction Guidelines

1. Purpose

This document outlines the importance of having a consistent and well understood password policy across the organization and its partners. The established policy takes into consideration various factors, including standards, industry best practices and practicality of implementation in the context of Parablu Inc..

At no point should any of Parablu Inc.' employees, contractors, vendors, partners become a victim of a password breach or a conduit to any incident arising from violation of established password policies. It is with this intent that this policy looks to ensure awareness and compliance across all stakeholders.

2. Scope

The scope of this policy includes all personnel who have accounts to any of Parablu Inc.' resources (emails, systems, customer deployments, source code, etc.). This means all employees, contractors, vendors, partners, customers who have access to any Parablu Inc. owned or deployed systems that require passwords in any form, including from within source code should take cognizance and adhere to this policy.

3. Importance of Passwords

Security and data breaches are very common. Most times it is due to weak passwords, shared passwords, passwords in plain text, lack of frequent password resets. It is possible for malicious actors to decipher passwords using technology, with enough compute time – which is the reason Parablu Inc. recommends strong passwords – which are long and further protected using multi-factor authentication and brute force password attack prevention.

4. Enforcement

Parablu Inc. has chosen to implement systemic protection to ensure violations do not occur to the extent possible. This will be by way of password policy enforcement in password / authentication & authorization systems, code review practices, awareness programs (first time and periodically), posters and emails communicating these frequently and clearly to all stakeholders. Parablu Inc. may choose to use various engaging methods to build security awareness and compliance – by way of videos, quizzes, incentives, security drills using automated tools.]

It is the responsibility of the end user to ensure enforcement with company policies. If you believe your password may have been compromised, please immediately report the incident to IT services and change the password (or request for your password to be changed).

5. Penalties

Any incident arising out of a violation of the policy will trigger investigation. Any personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Use of Passwords

Passwords or Secrets are attached to users (individuals), Systems, and Programs. They may be attached to programs / applications and systems that are automated. For programmatic access, embedding of passwords in source code or stored in configuration files is not allowed – instead, store these in key vaults and leverage service principals for systems.

7. Password Creation and Deletion

- Complex passwords should have password phrases of a minimum length of 14 characters which can include space, special characters, and numerals.
- Password should not be the same as the user id.
- Passwords should be unique per system. It should not be used for any personal accounts, other systems, or applications.
- Default passwords should be changed immediately upon first login.
- Enable Two-Factor Authentication or Multi-Factor Authentication (2FA, MFA) for all users.
- Enable Brute force password attack protection such reCAPTCHA to thwart automated/iterative password cracking attacks.
- Default system passwords on systems should be changed after completion of installation.
- All user ids and passwords that are no longer required should be disabled and deleted immediately. This should be requested formally via an authorized form via an authorized supervisor; request must be documented for traceability.

8. Password Protection

- Passwords should never be shared in any form (even with co-workers, supervisors) to ensure an accurate audit-trail and any inadvertent leaks.
- Passwords should not be revealed or transmitted electronically.
- Passwords shall not be written down or physically stored anywhere in the office and never at your work desk / systems.

- Do not store passwords electronically, in plain text – should always be kept encrypted. If they have to be stored/recorded, that should be done in encrypted files which require a complex password for access.
- When configuring password "hints," do not hint directly at the format of your password (e.g., "zip + middle name")
- User IDs and passwords must not be stored in an unencrypted format.
- User IDs and passwords must not be scripted to enable automatic login.
- "Remember Password" feature on websites and applications should not be used.
- All mobile devices that connect to the company network must be secured with a password and / or biometric authentication and must be configured to auto-lock within 5 minutes of inactivity.
- If someone requests for a password known to you, refer the person to this policy and have them contact an authorized system administrator to be granted access.
- Do not reveal passwords over the phone (this could be a social engineering attack). Note down the name and phone number of the person and notify your IT team.
- Be wary of login pages and screens that look very similar to the authentic pages. Verify that you are at the authorized secured page and system prompts.

9. Application Development Standards

(It is required that application developers follow company coding standards, recommended by OWASP-10). Application developers must ensure their programs contain the following security / credentials authentication precautions:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide role management, such that one user can take over the function of another without having to know the other's password.
- Remote Access Users Access to the company or customer networks via remote access is controlled using either a Virtual Private Network (in which a password and user id are required)

10. Deployment / Customer Installation

- Automate Password and Key generation – limit / eliminate humans from knowing these passwords and keys.
- Store in an encrypted form / Password protected, hashed and not retrievable to humans.
- Script and implement programmatic generation and retrieval. As far as possible deploy with safeguards such as Multi-factor authentication and brute force password attack protection activated.
- All underlying trusted programs should securely retrieve passwords/keys only at the time of access and not retain it in memory or other files.
- Installation and Deployment script should be automated end to end to use passwords and keys.
- Encourage customers to populate Parablu's SALT key to customize and randomize their user encryption keys for backup.

11. Password Auditing

The company may, at any time, choose use automated tools and personnel to guess and crack passwords. This is to ensure strong adherence to the policy and possible enhancement of the policy. If a password is guessed or cracked, corresponding individuals will be notified and asked to change the passwords immediately.

12. Contact / Emergency Contact

Emergency Contact for any suspected activity or breach must be reported immediately to itsupport@parablu.com.

For any clarifications or suggestions to this policy, please contact the CISO / Information Security department of Parablu Inc.

Software Installation Policy

1. Overview

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

2. Purpose

The purpose of this policy is to outline the requirements around installation software on Parablu Inc. computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Parablu Inc.'s computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3. Scope

This policy applies to all Parablu Inc. employees, contractors, vendors, and agents. This policy covers all computers, servers, smartphones, tablets, and other computing devices operating within Parablu Inc.' and its customer deployments.

4. Policy

- Employees may not install unauthorized software on Parablu Inc.'s computing devices operated within the Parablu Inc.'s network.
- Requests for software not on the authorized list must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email.
- Software must be selected from the approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.
- The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

Access Management Policy

1. Overview

Parablu Inc. establishes specific requirements for protecting information and information systems against unauthorized access.

2. Purpose

The purpose of this policy is to define required access control measures to all Parablu Inc. systems and applications to protect the privacy, security, and confidentiality of resources of Parablu Inc. and its customers. Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important, asset of Parablu Inc. which

must be managed with care. All information has value to the Organization. However, not all of this information has equal value or requires the same level of protection. Access controls are put in place to protect information by controlling who has the right to use different information resources and by guarding against unauthorized use. Formal procedures must control how access to information is granted and how such access is changed. This policy also mandates a standard for the creation of strong passwords, their protection, and frequency of change.

3. Scope

This policy applies to those responsible for the management of user accounts or with access to shared information or network devices, or physical areas. Such information can be held within a database, application, or shared file space. This policy covers all accounts, at all times, used for the purpose of business for Parablu Inc. and its customers; and applies to anyone associated with the organization with any form of access to Parablu Inc. and its customers' resources or information in any format, and on any device.

This policy applies to specific systems that, from an access standpoint, have significant implications to Parablu Inc.'s ability to render its service commitments.

Parablu Inc. is a software as a service (SaaS) company. As a SaaS company, the systems critical to achieve our service commitments include:
1. Production Infrastructure: Systems that run our software in order to provide our service
2. Change Management: Systems that store, version, and track changes to the source code of our software
3. Official Email: We rely on our official email for both internal and external official communication.

4. Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorization and clearance, may intentionally or accidentally gain unauthorized access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk. Non-compliance with this policy could have a significant effect on the efficient operation of the Organization and may result in financial loss and an inability to provide necessary services to our customers.

5. Definitions

- Access - The ability to use, modify or manipulate an information resource or to gain entry to a physical area or location.
- Access Control - The process of granting or denying specific requests for obtaining and using information. The purpose of access controls is to prevent unauthorized access to IT systems.
- Availability - Protection of IT systems and data to ensure timely and reliable access to and use of information to authorized users.
- Confidentiality - Protection of sensitive information so that it is not disclosed to unauthorized individuals, entities, or processes.
- Principle of Least Privilege - Access privileges for any user should be limited to resources absolutely essential for completion of assigned duties or functions, and nothing more.
- Principle of Separation of Duties - Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

6. Applying the Policy – Employee Access

6.1 User Access Management

Formal user access control procedures must be documented, implemented, and kept up to date for each application and information system to ensure authorized user access and to prevent unauthorized access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.
- User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated.
- System administration accounts must only be provided to users that are required to perform system administration tasks.

All privileged accounts (root, super user, and administrator passwords for servers, databases, infrastructure devices and other systems) must adhere to the requirements listed above and where possible and appropriate:

- Support authentication of individual users, not groups
- Configure devices with separate accounts for privileged and unprivileged access.
- Authenticate users with an unprivileged account rather than a privileged account.

6.2 User Registration and Revocation

A request for access to the Organization's computer systems must first be submitted to the IT Department for approval. Applications for access must only be submitted if approval has been obtained from the manager or function head.

When an employee leaves the organization, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager and function head of the person.

Organization and departments should maintain a running list of all resources and users, entities that have access to them. This list should be reviewed frequently (suggested – quarterly) and when personnel changes occur in their purview. Organization should use an onboarding and exit checklist along with status of granting or revoking access to resources per individual.

6.3 User Responsibilities

It is a user's responsibility to prevent their user ID and password is used to gain unauthorized access to Organization systems by:

- Following the Password Policy
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing IT department and their manager of any changes to their role and access requirements.

6.4 Principle of Least Privilege

Under least privilege, a staff member should only be granted the minimum necessary access to perform their function. An access is considered necessary only when a Parablu Inc. staff member cannot perform a function without that access. If an action can be performed without the requested access, it's not considered necessary. Least privilege is important because it protects Parablu Inc. and its customers from unauthorized access and configuration changes and in the event of an account compromise by limiting access.

Staff Access to Parablu Inc. Systems
1. Acceptable Usage Policy must be accepted by an employee before being granted access to systems that contain customer data. This policy outlines responsibilities and commitments regarding the acceptable use of the company's assets.
2. Access to Parablu Inc. systems will be granted on a need basis. The needs are dependent on the roles and responsibilities of a staff member, and the requirements to perform their duties effectively.
3. By default, Parablu Inc. staff members are granted access to Parablu Inc. systems according to their role and/or team. Ability to grant access to systems is restricted to administrators of each system.
4. If a Parablu Inc. staff member requires access outside of the default for their role or team, either they or their managers may request additional access to the administrators of the respective systems.
5. The system administrator evaluates the request and makes a decision regarding the access request. When granting such access, the administrator will limit the granted access to the minimum level that allows the requestor to perform the intended business operation.
6. Managers must notify the management or HR if a Parablu Inc. staff member has been terminated, or if their role or team has changed.

6.5. Segregation of Duties

Access privileges granted to each individual user will adhere to the principles of separation of duties. Technical or administrative users, such as programmers, system administrators, database administrators, security administrators of systems and applications must have an additional, separate end-user account to access the system as an end-user to conduct their personal business.

6.6 User Authentication for External Connections

Where remote access to the network is required, an application must be made via the IT department. Remote access to the network must be secured by two-factor authentication consisting of a username and one other component the authorized user alone possesses.

6.7 Supplier's Remote Access to the Organization Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Organization's network without permission from a senior company executive. Any changes to the supplier's connections must be immediately sent to the IT department so that access can be updated or terminated. All permissions and access methods must be controlled by IT department or Engineering department.

6.8 Operating System Access Control

Access to operating systems is controlled by a secure login process. The login procedure must also be protected by:

- Not displaying any previous login information e.g., username.
- Limiting the number of unsuccessful attempts and locking the account, if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorized users are allowed.
- All-access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g., administration rights). System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

6.9 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The 'business owner' of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with User Access Management and Password Policy.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorized higher levels of access.
- Be logged and auditable

7. Non-compliance

Parablu Inc. staff who violate this policy may face repercussions in proportion to the impact of their violation. Parablu Inc. management will determine how serious a staff member's offense is and decide the appropriate penalty. Penalties may include

Reprimand.
Demotion.
Suspension or termination for more serious offenses.
Detraction of benefits for a definite or indefinite time.

Acceptable Encryption Policy

1. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2. Scope

This policy applies to all Parablu Inc. employees and affiliates.

3. Policy

3.1 Algorithm Requirements

3.1.1 Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

3.1.2 Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

3.2 Hash Function Requirements

In general, Parablu Inc. adheres to the NIST Policy on Hash Functions.

3.3 Key Agreement and Authentication

3.3.1 All Asymmetric Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

3.3.2 Symmetric encryption algorithm should be AES-256

3.3.3 All on-the-wire transfers should minimally use TLS 1.2 with strong ciphers.

3.3.4 End points must be authenticated prior to the exchange or derivation of session keys.
3.3.5 Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
3.3.6 All servers and applications using TLS1.2 must have the certificates signed by a known, trusted provider.

3.4 Key Generation

3.4.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
3.4.2 As far as possible, avoid storing cryptographic keys and have them be generated and present in memory only for the period of the encryption/decryption operation.
3.4.3 Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

3.5 Note on Parablu's key management strategy

Parablu's key management method doesn't store or persist the keys anywhere. The keys are generated on-demand when required for encryption or decryption, used only when resident in computer memory and destroyed immediately afterwards. What Parablu persists in its database catalog is what we call a nonce or 'salt'. This is a long random string that can be chosen by the customer and changed at any time in the Parablu administrative console. It is not a password that needs to be memorized or written down. It just has to be a long and random string of alphanumeric characters – the longer and more random the better. The nonce is one of the ingredients used by our algorithm to generate user specific keys for encryption decryption. By simply changing the nonce, the administrator essentially causes all user keys to be re-generated.

4. Related Standards, Policies and Processes

National Institute of Standards and Technology (NIST) publication FIPS 140-2,
NIST Policy on Hash Functions

Router and Switch Security Policy

1. Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Parablu Inc. or its installations for customer.

2. Scope

All employees, contractors, consultants, temporary and other workers at Parablu Inc. and its subsidiaries must adhere to this policy. All routers and switches connected to Parablu Inc. production networks are affected.

3. Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentications.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled:
    a. IP directed broadcasts.

   b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses.
   c. TCP small services
   d. UDP small services
   e. All source routing and switching.
   f. All web services running on router.
   g. Discovery protocol on Internet connected interfaces.
   h. Telnet, FTP, and HTTP services
   i. Auto-configuration
4. The following services should be disabled unless a business justification is provided:
   a. Discovery protocol and other discovery protocols
   b. Dynamic trunking
   c. Scripting environments, such as the TCL shell
5. The following services must be configured:
   a. Password-encryption (#point 2)
   b. NTP configured to a corporate standard source.
6. All routing updates shall be done using secure routing updates.
7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
9. Access control lists for transiting the device are to be added as business needs arise.
10. The router must be included in the corporate enterprise management system with a designated point of contact.
11. Each router must have the following statement presented for all forms of login whether remote or local:
    "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."
12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbours. Password hashing for the authentication string must be enabled when supported.
14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    a. IP access list accounting
    b. Device logging
    c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped.
    d. Router console and modem access must be restricted by additional security controls.

Server Security Policy

1. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about getting the basics right.

2. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Parablu Inc. Effective implementation of this policy will minimize unauthorized access to Parablu Inc. proprietary information and technology.

3. Scope

All employees, contractors, consultants, temporary and other workers at Parablu Inc. and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated by Parablu Inc.

4. Policy

4.1 General Requirements

All internal servers deployed at Parablu Inc. or its customers must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs, and approved by the InfoSec team. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the InfoSec team. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up to date.
- Configuration changes for production servers must follow the appropriate change management procedures.

For security, compliance, and maintenance purposes, Parablu Inc. may monitor and audit equipment, systems, processes, and network traffic.

4.2 Configuration Requirements

- Operating System configuration should be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental backups will be retained for at least 1 month.
- Weekly full backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

Database Credentials Coding Policy

1. Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

2. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Parablu Inc.'s networks.

Software applications running on Parablu Inc.’s networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

3. Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on Parablu Inc.’s or its customers’ network. This policy applies to all software (programs, modules, libraries, or APIs that will access a Parablu Inc. production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they do not always use sanitized information.

4. Policy General

To maintain the security of Parablu Inc. databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

4.1 Specific Requirements

Storage of Data Base Usernames and Passwords

- Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must store the credentials encrypted and not be world readable or writeable.
- Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the Password Policy.

4.2 Retrieval of Database Usernames and Passwords

- If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use and decrypted programmatically for use. Immediately following database authentication, the memory containing the username and password must be released or cleared.
- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browse-able or executable file directory tree in which the executing body of code resides.

4.3 Access to Database Usernames and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the Password Policy.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Information Logging Standard

1. Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed daily, it is critical to have from a forensics standpoint.

2. Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

3. Scope

This policy applies to all production systems on Parablu Inc.'s and its customer deployment networks.

4. Standard

4.1 General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including where or on what system the activity was performed from (subject)?
- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was the activity was performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

4.2 Activities to be logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

- Create, read, update, or delete confidential information, including confidential authentication information such as passwords.
- Create, update, or delete information not covered in #1;
- Initiate a network connection.
- Accept a network connection.
- User authentication and authorization for activities covered in #1 or #2 such as user login and logout.
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes.
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes.
- Application process startup, shutdown, or restart.

- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3 Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

- Type of action – examples include authorize, create, read, update, delete, and accept network connection.
- Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
- Identifiers (as many as available) for the subject requesting the action – examples include username, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized to facilitate log correlation.
- Before and after values when action involves updating a data element, if feasible.
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
- Whether the action was allowed or denied by access-control mechanisms.
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4 Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Logs created directly by the source code are generated using syslog format and are managed using Log4j. Audit history for customer consumption shall be recorded in the Mongo meta-db for consumption via web-browser or via download as xls/xlsx by customer administrators. All efforts are made to ensure logs are tamper-proof, immutable and access restricted to only those who need it for specific reasons for solution maintenance or remediation.

4.5 Log Retention

As a company policy, all logs must be maintained for a minimum of 1 year. If a customer requires logs to be maintained for longer as per SLA agreed with them, that must be adhered to.

Web Application Security Policy

1. Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

2. Purpose

The purpose of this policy is to define web application security assessments within Parablu Inc.. Web application assessments are performed to identify potential or realized weaknesses as a

result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Parablu Inc.'s services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Parablu Inc..

All web application security assessments will be performed by delegated security personnel either employed or contracted by Parablu Inc. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of Parablu Inc. is strictly prohibited unless approved by the CISO.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. Policy

4.1 Web applications are subject to security assessments based on the following criteria:

- New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
- Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the CISO or an appropriate senior company executive who has been delegated this authority.

4.2 All security issues that are discovered during assessments are mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

- High – Any high-risk issue must be fixed immediately, or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high-risk issues are subject to being taken off-line or denied release into the live environment.
- Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly. This could also result in being denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level.

The following security assessment levels have been established by the InfoSec organization

- Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide.
- Quick – A quick assessment using a tool such as OpenVAS or ZAP will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
- Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

5. Related Standards, Policies and Processes

OWASP Top Ten Project
OWASP Testing Guide
OWASP Risk Rating Methodology

Risk Assessment, Impact and Treatment Policy

1. Overview

Risk Assessment is the first step in documenting and scoring all possible risks across various workflows and functions of Parablu Inc.

2. Purpose

The purpose of this policy is to facilitate compliance with applicable federal and state laws and regulations, assimilate industry best practices to protect the confidentiality and integrity of Parablu Inc, procurement, personnel, product-solution development, testing, infrastructure, and customer deployment; and enable informed decisions regarding risk tolerance and acceptance.

3. Policy

This IT policy, and all policies referenced herein, shall apply to all members of the company and partners who use, access, resources, sensitive information, implement infrastructure, implement, and deploy solutions for Parablu and its customers.

- The company and different groups are required to perform periodic information security risk assessments to determine areas of vulnerability and to initiate appropriate remediation.
- The company uses formal Information Security Risk Management (ISRM) programs that identify risks and implement plans to address and manage them.
- The Information Security group is responsible for managing the Information Security Risk Management program and coordinating the development and maintenance of program policies, procedures, standards, and reports.
- Risk assessments must identify, quantify, and prioritize risk acceptance and objectives relevant to the company and its operations. The results are to guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls to protect against these risks.
- The risk assessment must include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the calculated risks against risk criteria to determine the significance of the risks (risk evaluation). Have assigned Owners who will be accountable to mitigate the identified risks according to agreed mitigation steps.

- Risk assessments are performed periodically to address changes in security requirements and the risk situation (e.g., threats, vulnerabilities, impacts, risk evaluation, and data classification).
- Risk assessments are to be undertaken systematically, capable of producing comparable and reproducible results. The information security risk assessment should have a clearly defined scope to be effective and should include relationships with risk assessments in other areas, if appropriate.
- Risk Reporting – the company will use a risk log or register to assist with documenting the identified risks and their status. The report shall be presented and reviewed / approved periodically (recommended at time of major release or at least once a year) to provide a view of the strategic and operational risks identified and the steps taken to mitigate the risk.
- Response - The appropriate response will be based upon identified risk tolerance levels – remediate, mitigate, transfer, accept, or avoid. Plans will be developed and response to the risk will be assigned to respective functional groups to take steps to reduce risk to an acceptable level. Cooperation from all functions will be required to reduce risk in the environment. These steps will be monitored, tracked in the risk register, tested, and reported to senior leadership.
- Performance – Risks should be reduced quarterly, completing and reporting progress on plans in accordance to compliance requirements. Information Security incidents that are investigated and analyzed for risk resulting in the appropriate response or controls implemented.
- Tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

4. Risk Acceptance Criteria

- Risk values 0 through 2 are acceptable risks.
- Risk values 3 and 4 are unacceptable risks. Unacceptable risks must be treated.

5. Risk Treatment

- Risk treatment is implemented through the Risk Treatment Table. All risks from the Risk Assessment Table must be copied to the Risk Treatment Table for disposition, along with treatment options and residual risk.
- As part of this risk treatment process, the CEO and/or other company managers shall determine objectives for mitigating or treating risks. All unacceptable risks must be treated. For continuous improvement purposes, company managers may also opt to treat other risks for company assets, even if their risk score is deemed to be acceptable.
- Treatment options for risks include the following options:
- Selection or development of security control(s).
- Transferring the risks to a third party; for example, by purchasing an insurance policy or signing a contract with suppliers or partners.
- Avoiding the risk by discontinuing the business activity that causes such risk.
- Accepting the risk; this option is permitted only if the selection of other risk treatment options would cost more than the potential impact of the risk being realized.
- After selecting a treatment option, the risk owner should estimate the new consequence and likelihood values after the planned controls are implemented.

6. Sample Reporting

This is a sample risk assessment, scoring, treatment. Refer to the formal Risk Register maintained by the company. The results of risk assessment and risk treatment, and all subsequent reviews, shall be documented in a Risk Assessment Report.

Description of Consequence Levels and Criteria

Consequence Level	Consequence Score	Description
Low	0	Loss of confidentiality, integrity, or availability will not affect the organization's cash flow, legal, or contractual obligations, or reputation.
Moderate	1	Loss of confidentiality, integrity, or availability may incur financial cost and has low or moderate impact on the organization's legal or contractual obligations and/or reputation.
High	2	Loss of confidentiality, integrity, or availability will have immediate and or/considerable impact on the organization's cash flow, operations, legal and contractual obligations, and/ or reputation.

Description of Likelihood Levels and Criteria

Likelihood Level	Likelihood Score	Description
Low	0	Either existing security controls are strong and have so far provided an adequate level of protection, or the probability of the risk being realized is extremely low. No new incidents are expected in the future.
Moderate	1	Either existing security controls have most provided an adequate level of protection or the probability of the risk being realized is moderate. Some minor incidents may have occurred. New incidents are possible, but not highly likely.
High	2	Either existing security controls are not in place or ineffective; there is a high probability of the risk being realized. Incidents have a high likelihood of occurring in the future.

Patch and Vulnerability Management

1. Patch Management

- The Organization IT team maintains overall responsibility for patch management implementation, operations, and procedures.
- All Information Resources are scanned on a regular basis to identify missing updates.
- All missing software updates are evaluated according to the risk they pose to Organization.
- Software updates and configuration changes applied to Information Resources are tested prior to widespread implementation and must be implemented in accordance with the Organization Change Control Policy.
- Critical Patches are identified on a quarterly basis and are first applied to Internal Dev/QA systems for verification.
- Once verified, such patches are then applied to Pre-Production (Dogfood lab) systems and only after successful verification - rolled out to Production setups.
- Verification of successful software update deployment will be conducted within a reasonable time period as defined in the Organization Patch and Vulnerability Standard.

Network Security

There is no single definitive mechanism for completely protecting a network because, virtually, any security system can be compromised or subverted. Intrusions may be from outside or internally orchestrated. Therefore, the most effective way to secure a network system may be by implementing different layers of security barriers. This makes an attacker must bypass more than one system to gain access to critical assets of the target.

1. Servers and Network – Security hardening processes

- Network firewall protection
- VPN is enabled for the User outside the organization with ACL
- Host firewall enabled using UFW/Iptables
- Host based web-application firewall protection
- Host based anti-malware
- Host based intrusion detection
- Port Obfuscation for well known ports
- No root access – just-in-time privilege escalation
- Complex password enforcement
- Multi-factor authentication
- Always-ON SSL
- Valid SSL Certificates

Capacity and Performance

Parablu Inc., monitors all test, production, and POC servers 24x7 using call-home alerts. This acts as a capacity planning tool as well as feeds a dashboard for real-time reporting and analytics.

https://opcenter.parablu.com

Alert monitoring via support@parablu.com

Business Continuity and Disaster Recovery Policy

1. Purpose

The purpose of the Business Continuity Policy is to provide an effective documented framework and a process to manage critical activities & their dependencies in case of an emergency.

The objectives of the Business Continuity & Disaster Recovery Policy are:

- To mitigate the possible impact of an interruption to the activities
- To recover processes at identified recovery facilities
- To be able to resume business as usual post the interruption or disaster

2. Scope

The Business Continuity Policy does not address specific disaster events; it is written for a generic situation, which assumes that the primary site is suddenly inaccessible or must be vacated without warning.

Business Continuity & Disaster Recovery Plan

1. Scope

There are three primary aspects to a business continuity plan for key applications and processes:

- **High availability**: Provide for the capability and processes so that a business has access to applications regardless of local failures. These failures might be in the business processes, in the physical facilities or in the IT hardware or software.
- **Continuous operations**: Safeguard the ability to keep things running during a disruption, as well as during planned outages such as scheduled backups or planned maintenance.
- **Disaster recovery**: Establish a way to recover a data center at a different site if a disaster destroys the primary site or otherwise renders it inoperable.

Parablu Inc.'s Disaster recovery strategy is designed to provide resources needed to:

- Minimize risk.
- Resume operations quickly.
- Maintain industry compliance.
- Address concerns of employees, owners, and investors.

2. Enforcement

Parablu Inc., computing systems are hosted in data centers which are separated from the office's physical locations. Employees can access these systems from outside the office without any need for office infrastructure. Any disaster striking the office will have little or no impact on continuing business operations.

All the Production workloads like mail, file services, conferencing etc. are hosted using Microsoft 365 services. Source code, bug-database, support-ticketing etc. are all hosted in cloud workloads such as Git, Bugzilla, and OSTicket. Parablu's company website is hosted on Microsoft Azure.

Customer workload hosting is done using vendors such as Linode and Oracle Cloud. Dev/Test workloads are hosted using AWS and Digital Ocean. All these partners have world-class data centers with a geographical spread. An isolated incident even in any one of these data centers can easily be mitigated by migrating workloads elsewhere.

All production and customer workloads have frequent up-to-date backups which enable Parablu Inc. to stand-up the same workload in an alternate data center in < ½ a working day.

Any changes involving customer workloads – either due to hardware maintenance or due to software patch management which involves downtime amounting to greater than 5-10 minutes – will be communicated as "planned maintenance outage" to customers ahead of time.

Incident Management

To reduce the impact of information security breaches, Parablu Inc., ensures that incidents are followed up correctly. Incident management is designed to help identify areas for improvement to decrease the risk and impact of future incidents.

1. Policy Statement

The purpose of this Policy is to ensure that any incidents that affect the daily operations are managed through an established process.

All Employees have an important part to play in reporting and managing information security incidents to mitigate the consequences and reduce the risk of future breaches of security.

This Policy provides a framework for reporting and managing:

- Security incidents affecting the Council's information and ICT systems.
- Losses of information
- Near misses and information security concerns

2. Scope

The incident management strategy adopted by Parablu Inc., comprises the following broad steps:

1. Stop the breach - This is done by isolating the systems (or IPs, user logins etc.) which are compromised, from the rest of the network. We then work to identify the vulnerability the attacker may have used to infiltrate and plug that vulnerability immediately. We cleanse the compromised assets - before allowing for them to re-enabled or re-used.

2. Damage assessment - we then take stock to see what (if any) data got compromised. How sensitive or high-risk it was, and whether the data was encrypted. And if the data was damaged, how quickly it can be restored. We also study the attack vector, what techniques the attacker may have used to gain access so we can take steps to mitigate.

3. Notification - based on the information we gain through the above process; we will notify stakeholders involved, such as customers, partners or government authorities - so they get an accurate understanding for what data was compromised and what the risk is due to such a compromise.

4. Security Audit - we will then perform a full security audit and re-examine all our processes and safe-guard and update them as required.

Third Party Risk Management Policy

1. Policy

The purpose of the TPRM policy is to establish and communicate the standards and guidelines for all employees and contractors who work with third-parties such as vendors or suppliers that support internal functions and processes.

2. Exception to the TPRM process

As a general rule, Parablu Inc., will not outsource any core or critical functions to third-parties. In case an exception is made to such a rule, a TPRM assessment is required. The level of criticality associated with the outsourced functions and processes will determine whether a TPRM assessment is required. The level of criticality should be determined by the InfoSec team and the CISO after studying the details of the function and detailed interviews with the third-party.

3. Essential policies for vendor management

All vendor contracts will have these clauses addressed to the satisfaction of Parablu Inc.

- Service level agreements (SLAs)
- Vendor compliance standards
- Acceptable vendor controls
- Vendor liability in the event of a data breach

- Termination of contract when security requirements are not met
- Board or senior management oversight where needed
- Disaster recovery and established redundancies for important business functions

During the process of onboarding a vendor, Parablu Inc. will determine whether the level of access each vendor requests makes sense. Not all vendors require the same level of access to sensitive data, network, and information technology systems to do their job.

Physical Security

1. Policy Statement

To meet enterprise business objectives and ensure continuity of operations, Parablu shall adopt and follow well-defined and time-tested plans and procedures, to ensure the physical security of all information assets and human assets. Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including personnel and information security. A balanced security program must include a solid physical security foundation. A solid physical security foundation protects and preserves information, physical assets, and human assets.

2. Purpose

The purpose of the Physical Security Policy is to:

- Establish the rules for granting, control, monitoring, and removal of physical access to office premises;
- Identify sensitive areas within the organization, and protect them via biometric authentication methods
- Define and restrict access, as necessary.

3. Scope

- All physical security systems comply with applicable regulations including but not limited to building codes and fire prevention codes.
- Biometric Authentication to the main entrances as well as sensitive locations like labs containing servers and networking equipment.
- Employees and visitors are required to provide proof with an employee or visitor ID if requested to do so.
- Visitors should always be accompanied / escorted by an Employee host for the period of their visit.
- Employees are encouraged to question and challenge any visitor or vendor who has gained access and is unescorted to produce a positive ID.
- All employees and visitors are temperature checked each day
- Only employees and visitors with at least 2 weeks of time elapsed post their vaccination for COVID-19 are allowed into the premises.
- Attendance log

Human Resource Security

1. Recruitment and selection

Parablu Inc., follows a multi-level candidate selection and interview process to identify qualified applicants per the job description published by our business teams. We ensure that we select the right candidate who not only satisfies the job requirements, but also evaluate the candidate holistically

to ensure that they contribute positively to the company's innovation driven culture and are given the opportunity to play a pivotal role in the sustenance and growth of our business.

2. Background Verification

Checks are performed prior to the employee's joining date, to confirm education, employment history, non-existence of a criminal record, and other activities from their past.

We also perform reference checks from a previous employer – preferably from at least 2 former supervisors.

In the event of suspicious activity, or if Parablu deems necessary, Parablu reserves the right to repeat the above checks and update our records.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
Additionally, the company may at its discretion seek legal remedies for damages incurred because of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

3. Supporting document verification

- Proof of Education
    - Transcripts, Marks cards, and or educational certificates.
- Last Company Relieving Letter / Pay-Slips / IT Declarations
    - Pay-slips covering the previous 3months of employment / Relieving Experience Letter & copies of Income Tax Declarations.

4. Training

New employees are provided with the Company handbook, the Information Security Policy (this document) and the POSH handbook – which they must read and acknowledge.

Parablu Inc. adopts the PoSH (Prevention of Sexual Harassment)" policy which is designed to infuse in employees, a culture in which women and minorities can feel safe in a working environment. An online training and test are conducted on a yearly basis to ensure compliance.

5. Employee Agreement

The Employment Agreement is a contract we enter when the business hires a new employee. This Agreement sets out all of the terms of employment, including Job duties, Salary, Benefits, work hours, Confidentiality of Company and Customer data, Intellectual Property policy, Annual leave and various other key parameters.

6. Employee Relieving Process

7. Exit Interview

The purpose of an exit interview is to assess the overall employee experience within Parablu Inc. and identify opportunities to improve retention and engagement.

8. Disabling access

Access to all company resources is terminated – including but not limited to email, source code control system, bug database, support database, server access, other third-party SaaS tools etc. All email communication is auto forwarded to the respective reporting manager.

9. Collecting back the company assets

All company property (like laptop(s), mobile access points, books, documentation, company ID, key cards etc.) retrieved from the relieving employee.

The employee is blocked from the Biometric database preventing admission to the office premises – and the physical security team is notified of their departure.

10. Relieving letter

A relieving letter / experience letter along with a Full and Final settlement of due salary is provided to the employee only upon satisfactory completion of all the above steps.

File sharing Policy

Scope

File sharing and collaboration - any file sharing, managed file transfer or collaboration needs to be performed exclusively using Parablu's BluSync™ solution, which is designed to protect data both during transit (using TLS 1.2 with strong ciphers), and at rest (using AES-256 encryption).

Non-compliance

Compliance with this policy will be verified through various methods, including but not limited to, automated reporting, audits, and feedback to the policy owner.

Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment, or contractual agreement. The action will depend on the extent, intent and repercussions of the specific violation(s).

Information Classification, handling & labelling:

Data classification provides a way to categorize data processed by Parablu Inc., its software and systems, based on levels of sensitivity. The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to the organization. By understanding the types of available data, its classification and access level, you can map the appropriate access/protection of the data. This ensures that sensitive corporate and customer data can be secured appropriately.

Scope

The Parablu Inc. Data Classification Policy applies to all data handled, managed, stored, or transmitted by Parablu Inc. and Parablu Inc. staff. Managers and/or information owners are responsible for assigning the appropriate classification as and when required.

Roles and Responsibilities

Everyone at Parablu Inc. is responsible to review, adhere to and handle data according to the classification levels below. The Data Classification definitions (described below) provide a list of various types of data and their classification level. If you cannot identify the data element or are uncertain of the risk associated with the data and how it should be classified and handled, please contact the Information Security Officer.

Data Classification Definitions

We classify data into the following types

1. Public

This is data or information that can be shared with any person, organization, system regardless of their relationship with Parablu Inc.. This classification is not limited to data or information that is meant for public consumption, but includes any data or information that requires no special handling, or any kind of safeguarding from disclosure. Distribution of such data does not expose Parablu Inc., its

customers or its partners to any harm. Examples of public data: Product blog, Company product website, Press releases, Company marketing collateral, Careers page etc

2. Company classified

This is data and information that should not be made generally available. Unauthorized access or disclosure could cause significant or financial material loss, risk of harm to Parablu Inc. if exposed to unauthorized parties, break contractual obligations, and/or adversely impact Parablu Inc., its partners, employees, and eventually customers. Such information is to be protected from unauthorized accessor changes. Company classified data should only be accessible to pre-authorized staff members. Note that access to such data can also be limited to specific staff members or groups of staff members (like executives, human resources, legal teams etc).

Unauthorized access to company classified information could violate privacy policies, contractual agreements, cause security incidents, cause financial loss, crucial gains for competitors, and/or adversely impact Parablu Inc., its partners, staff.

Examples of Company classified data: Employee salaries, Legal documents, Internal product specifications, customer lists, Strategy documents, internal roadmaps, design documents, Internal memos or emails etc.

3. Customer classified

Customer classified data is one that if accessed by unauthorized parties may adversely affect Parablu Inc.'s customers. This includes data that Parablu Inc. is required to keep confidential, either by law or under a customer agreement. We have to protect such information from not just unauthorized access but also unauthorized modification. Customer-classified data should be safeguarded both when it is stored as well as being processed/used/transmitted.

Unauthorized access to such data can potentially violate contractual confidentiality agreements with customers, cause a security incident, or affect Parablu Inc.'s customer and industry confidence.

Examples of Customer classified data: Information provided by customers by the way of using our system, information of users of customer accounts, personally identifiable information of customers (or customer’s customers) etc.

Acceptable Usage and Bring Your Own Device (BYOD) Policy

Parablu Inc. is committed to safeguard the information and other assets shared with us by our customers, partners, and staff. They depend on us to protect their resources. Thus, it is crucial for all Parablu Inc. staff to understand how to responsibly use our systems such that we can protect the security, availability and confidentiality of such assets.

Principle & Purpose

Parablu Inc. has a culture of trust and integrity. This policy aims to reinforce the trust we place in each other, by ensuring we can collectively depend on each other to protect the assets of our staff, company, partners and customers.

Security is a company-wide effort, and requires cooperation from every staff member who works with Parablu Inc. systems. Each individual must take precautions to ensure they use systems appropriately and do not, deliberately or inadvertently, perform damaging or illegal actions.

This policy does not intend to curb or hinder reasonable use of Parablu Inc. systems.

Scope:

This policy applies to all Parablu Inc. employees, contractors, consultants, temporary, and other workers that interact with Parablu Inc. systems. All such individuals are responsible for exercising good judgment to appropriately use electronic devices, data, and network resources in accordance with policies and standards, and local laws and regulation.

This policy applies to the use of

* Any company-issued electronic, computing, storage, or network device

* Any company owned systems on Internet / Intranet, including but not limited to servers, software, operating systems, storage, network accounts

* Any company administered accounts with third party services providing email, storage, infrastructure, software, data, APIs, business systems etc, irrespective of whether such accounts are accessed via devices owned/leased by the company, the staff member or a third party

Separation of concerns

Parablu Inc. staff are strongly encouraged to separate work activities from personal activities as much as possible.

Parablu Inc. staff are expressly prohibited from using non-company issued devices including, but not limited to laptops, desktops, tablets and mobile phones for any company related activity.

Parablu Inc. staff may use your company-issued devices for reasonable personal use, but those devices do not belong to you.

Specifically:

Parablu Inc. staff are encouraged to separate work activities from personal activities as much as possible.

Parablu Inc. staff may use your company-issued devices for reasonable personal use, but those devices do not belong to you. Specifically:

*Company administrators may have access to staff data when they are trying to repair/debug/troubleshoot our systems.

* Terminated employees' devices can be transferred to another employees, which may give them access to the terminated employees' data.

* In a scenario where the company is defending itself in a court of law, data on all company-issued devices are potentially accessible to opposing counsel.

* If case of a breach, outside investigators will likely inspect all use of an account and/or device.

To summarize, company-issued devices and accounts are not your personal property, and as a result, we strongly recommend limiting their use for personal reasons as much as possible. Non-company devices are expressly prohibited from use for any company related work.

Security and Proprietary Information

* All classified or proprietary data stored on computing and storage devices, whether owned or leased by Parablu Inc., the employee or a third party, remains the sole property of Parablu Inc..

* You must ensure that all classified or proprietary data is handled and protected in accordance with the Data Classification Policy

* You are required to promptly report the theft, loss or unauthorized disclosure of any classified /proprietary data

* You may access, use or share classified / proprietary information only to the extent it is authorized and necessary to perform your job responsibilities

* Staff members are responsible for exercising good judgment when using Parablu Inc. systems for reasonable personal use. If there is any uncertainty, staff should consult their supervisor or manager.

* Parablu Inc. reserves the right to audit any system at any time to ensure compliance with this policy. Authorized individuals within Parablu Inc. may monitor equipment, systems and networks at any time.

Unacceptable Use

Staff members may not use Parablu Inc.-managed resources for activities that are illegal or prohibited under applicable law, no matter the circumstances.

Staff members may not use any resources not managed or issued by Parablu Inc. for any company related activity.

Unacceptable System and Network Activities

Prohibited system and network activities include, but are not limited to, the following:

* Use of personal devices for company related work

* Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

* Unauthorized copying, distribution, or use of copyrighted material.

* Exporting software, technical information, encryption software, or technology in violation of international or national export control laws.

* Intentional introduction of malicious programs into Parablu Inc. networks or any Parablu Inc.-managed computing device.

* Intentional misuse of any Parablu Inc.-managed computing device or Parablu Inc. networks (e.g. For cryptocurrency mining, botnet control, etc.).

* Sharing your credentials for any Parablu Inc.-managed computer or 3rd party service that Parablu Inc. uses with others, or allowing use of your account or a Parablu Inc.-managed computer by others. This prohibition does not apply to single-sign-on or similar technologies, the use of which is approved.

* Using a Parablu Inc. computing asset to procure or transmit material that is in violation of sexual harassment policies or that creates a hostile workplace.

* Making fraudulent offers of products, items, or services originating from any Parablu Inc. Account.

* Intentionally accessing data or logging into a computer or account that the team member or contractor is not authorized to access, or disrupting network communication, computer processing, or access.

* Executing any form of network monitoring that intercepts data not intended for the team member's or contractor's computer, except when troubleshooting networking issues for the benefit of Parablu Inc..

* Circumventing user authentication or security of any computer host, network, or account used by Parablu Inc..

* Tunnelling between network segments or security zones (e.g., gprd, gstg, ops, ci), except when troubleshooting issues for the benefit of Parablu Inc..

Unacceptable Email and Communications Activities

Forwarding of confidential business emails or documents to personal external email addresses.

Note: Parablu Inc. may retrieve messages from archives and servers without prior notice if Parablu Inc. has sufficient reason to do so. If deemed necessary, this investigation will be conducted with the knowledge and approval of the Security, People Business Partners, and Legal Departments.

Communications and Operations Management Policy:

1. Policy

1.1 Operational Procedures and Responsibilities

1.1.1 Documented Operating Procedures

System Administrators will ensure operating procedures are used in all day to day maintenance of Parablu's systems and infrastructure in order to ensure the highest possible service from these assets. System Administrators will ensure these operating procedures are documented to an appropriate level of detail for the intended audience.

1.1.2 Change Management

The change control procedure should include:

- A description of the change and business reasons
- Information concerning the testing phase
- Impact assessment including security, operations and risk
- Formal approval process
- Communication to all relevant people of the changes
- Procedures for aborting and rolling back if problems occur
- Process for tracking and audit

1.1.3 Separation of Development, Test and Operational Facilities

The Parablu Technical Team will ensure the development and test environments are separate from the live operational environment to reduce the risk of accidental changes or unauthorised access. The environments must be segregated by the most appropriate controls including, but not limited to, the following:

- Running on separate computers, domains, instances, and networks.
- Different usernames and passwords.
- Duties of those able to access and test operational systems.

1.2 System Planning and Acceptance

1.2.1 Capacity Planning

The Parablu Technical Team will ensure all Parablu infrastructure components or facilities are covered by capacity planning and replacement strategies to ensure that increased power and data storage requirements can be addressed and fulfilled in a timely manner.

Key Parablu infrastructure components include, but are not restricted to, the following:

- Physical servers
- Domain servers
- Printers
- Networks
- Environmental controls including air conditioning

For customer workloads, capacity is monitored continuously via real time alerts which informs the Parablu SOC team of issues as related to disk, CPU or memory starvation - which are analyzed right away. Remedial action is usually taken in 24-48 hours depending on the severity of the capacity issue.

1.2.2 System Acceptance

Users and Services must ensure any new information systems, product upgrades, patches and fixes undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve management authorisation.

1.2.3 Protection against Malicious Attacks

The Parablu Technical Team will ensure all appropriate steps are taken to protect all Parabu systems, infrastructure and information against malicious code by running effective and up-to-date anti-virus software on all servers and PCs.

1.2.4 Patching

The Parablu Technical Team will ensure all servers have appropriate critical security patches applied as soon as they become available and have passed the system acceptance testing. All other patches must be applied as appropriate. Patches must be applied to all software on the Parablu network where appropriate.

The Parablu Technical Team will adhere to Parablu's Patch Management Procedure and keep a full record of which patches have been applied and when.

1.3 Backups

1.3.1 Information Backup

The Parablu Technical Team will ensure regular backups of essential business information are taken to ensure that the Parablu can recover from a disaster.

The Parablu Technical Team will ensure full backup documentation, including a complete record of what has been backed up along with the recovery procedure, is stored at two different location and be readily accessible.

The backup target must always be an offsite cloud location for purposes of geographical redundancy and DR.

1.3.2 Information Restore

The Parablu Technical Team will ensure full documentation of the recovery procedure is created and stored. Regular restores of information from back up media will be tested to ensure the reliability of the backup media and restore process and this should comply with the agreed change management process.

1.4 Security of System Documentation

System Administrators must ensure system documentation is protected from unauthorised access.

Effective storage version control should be applied to all documentation and documentation.

1.5 Monitoring

The Parablu Technical Team will ensure audit logs are kept for a minimum of six months which record exceptions and other security related events. As a minimum audit logs must contain the following information:

- System identity
- User ID
- Successful/Unsuccessful logon
- Successful/Unsuccessful logout
- Unauthorised application access
- Changes to system configurations

1.6 Protection of System Test Data:

System Administrators will ensure that If personal information is used during the development and test phase of preparing application software it is protected and controlled in line with the Data Protection Act and where possible depersonalised. If operational data is used controls must be used including, but not limited to, the following:

- An authorization process
- Removal of all operational data from the test system after use
- Full audit trail of related activities
- Any personal or confidential information must be protected as if it were live data

1.7 Annual Health Check:

The Parablu Infrastructure Manager will ensure an annual health check of Parablu's infrastructure systems and facilities is undertaken every 18 months. This health check must include, but is not restricted to, the following:

- A full penetration test
- A network summary that will identify all IP addressable devices

- Network analysis, including exploitable switches and gateways
- Vulnerability analysis, including patch levels, poor passwords and services used
- Exploitation analysis
- A summary report with recommendations for improvement

Definitions and Terms

Several of security definitions and terms referenced can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/