1. Overview

The purpose of this document is to formalize the security procedures to be followed by the technology team members at Wishes. This encompasses the product team engineering team and site-reliability/DevOps teams. It outlines standards that are hard requirements to keep processing, transmitting, and securing sensitive customer data, cardholder data and passwords and IDs.

2. Purpose and Objectives

The team member at Wishes must:

a. ensure that not only aware of all topics outlined here, but also that they're responsible to disseminate the knowledge acquired through this policy to their peers, to our customers, partners, and any other parties that are neglecting acceptable security standards both from a moral, ethical perspective, as well as from a legal and technical standpoint;

b. constantly make sure to follow risk assessment standards, by constantly evaluating impact through a strict change-control policy, planning sessions before implementing any new features, and that everything requested is properly documented, up-to-date and pristine from a rollback and disaster recovery standpoint;

c. respect infosec roles, and be truly accountable for their infosec responsibilities; and by that, serve and maintain the security team ;

d. disseminate information regarding best practices, new vulnerabilities, and engage on every single activity that can improve our security;

e. go over our security awareness program, to ensure all security matters are followed

f. participate on security events both funded by the company through our security events budget, and alert the company whenever valuable events are available;

g. be part of incident management and response process, through fast, assertive, communication, and thoughtful, well-designed and as close to permanent solutions as possible;

3. Risk Assessment and Reduction

Our risk assessment and reduction policy is based on three main factors:

a. Probability, which is the possibility of a vulnerability being exploited and becoming an actual threat; this possibility is defined through factual data, such as the general public exposure to this flaw;

b. Severity, which basically translates to how large the consequences on our information security are, if this is exploited. Our main factors are for scoring severity are confidentiality, integrity and availability;

c. Relevance, which is the level of importance from a business perspective, considering the components that would be exposed if exploited.

3.1. Risk Score

These three factors generate a risk score, which is the multiplication of these three factors,

scored from 1 to 5 by the Security team . This indicator presents the total risk that our resources are exposed in the case of a control measure not being implemented. Below we have represented what the values for each one of these cases are:

Risk Score	Risk Level	Definition
10	Very High	Unacceptable: must be resolved immediately
7	High	Worrisome: must be at least controlled and reduced
5	Medium	Alarming: must be formally notified and followed up
3	Low	Attention required: acceptable if kept controlled
1	Very Low	Acceptable: under control and must be kept that way

4. Critical Technology Usage and Approval

Employees of Wishes may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include personally owned cell phones, smartphones, tablets, laptops and computers. This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data using their personal device. This policy applies to, but is not limited to, any mobile devices owned by any users listed above participating in the Wishes BYOD program which contains stored data owned by Wishes, and all devices and accompanying media that fit the following device classifications: ● Laptops ● Tablets ● Mobile/cellular phones, including smartphones ● Any non-Wishes owned mobile device capable of storing corporate data and connecting to an unmanaged network The use of personal devices is limited to certain employees and may be limited based on compatibility of technology. Contact the CEO for more details.

Given that Wishes is a fully remote company, having offices across multiple countries and the majority of its employees distributed, there are certain definitions that rule and should be followed strictly in order to keep our intellectual property, client data and our cardholder data environment safe. These definitions include the following:

a. Given that the majority of the devices are owned by the employees, we don't use invasive methods, in terms of privacy, in their own environment; but it is extremely recommended that higher management, directors and executives use at least a well known anti-virus, endpoint protection or firewall software on their daily activities; if using systems that are known to be safer (such as Unix-like systems), this requirement is waived under approval by authorized parties;

- Chase Harmer:
    - Antivirus: Norton360, Trend micro
    - Firewall: Norton360
    - Password manager: Dashline

- Annie Rhodes
    - Antivirus: Norton360
    - Firewall: Norton360
    - Password manager: Dashline
- Alex Galert:
    - Antivirus: Kaspesky
    - Windows 11 firewall
    - Dashline password manager
- Max Popov
    - Antivirus: windows defender
    - Windows 11 firewall
    - Google chrome password manager
- Alex Gorin
    - Avast Ultimate (Multi-Device) Premium
    - Avast Firewall Premium
    - Dashline password manager
- Andrey Kolesnik
    - Antivirus: windows defender
    - Firewall: Windows 11 firewall
    - Password manager: Dashlane
- Vitaliy Borisov
    - Antivirus: windows defender
    - Firewall: Windows 11 firewall
    - Password manager: Dashlane

b. It is expected that these groups of people also use a password manager, such as Dashlane to manage their passwords, and have a different password for each service they do use. This prevents that in event of a leak of one of the services being used, only that specific account is exposed;

c. All documents, sensitive data and mission-critical information should never be stored on their local workstations, but in our Google Drive instead. This prevents us on the event of the security breach on a workstation, we first don't expose sensitive data to an attacker and secondly that by in the event of data loss, disaster recovery or similar, the data is stored on the cloud and we have easy access to it through a new device;

d. Sensitive data such as card numbers and account numbers should never be sent through IM through Hangouts, Slack or any other instant messaging or end-to-end technologies. This sort of sensitive information should be transmitted through phone, exclusively;

e. When accessing the CDE or critical systems from a different geographical location or network than usual, ensure that the security team is aware, just so in case of this access raising any flags, we're aware that one team member is actually on this location and we can consider it a false-negative instead of digging into it too much

with the hypothesis of unauthorized access;

f. Every single access done to any system s are properly done through your specific user account, with multi-factor authentication enabled, and not a generic one such as support@wishes.inc so we can clearly assign the correct user identification to the account, as not having clear identification may act as a back-door for an attacker;

g. No data from the cardholder environment should be saved to a local environment unless explicitly authorized and requested in written by a stakeholder, such as the CTO or the CEO; and this data should be completely wiped out, on an unrecoverable manner, right after it fulfills the expected need.

5. Personal Responsibilities

Our access to the Production and Staging environments is given under Asana ticket requests.

All operational roles are responsible for:

- Monitoring and analyzing security alerts and information, and distributing to appropriate personnel;
- Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations;
- Administering user accounts, including additions, deletions, and modifications;

6. Service Provider Management

Our business relies on a few service providers that have very critical access to our data. Our approach to our choices for partnerships relies on favoring two main criteria: companies that are industry leaders and companies that are specifically endorsed by the PCI council themselves.

6.1. www.hetzner.com

https://www.htezner.com
Hetzner is the lead cloud provider, offering Infrastructure and Software as a Service in compliance with PCI DSS, GDPR and more.

6.2. NMI Gateway

http://nmi.com/
By integrating four key technologies – tokenization, encryption, data vaulting, and key management – with a highly secure cloud-computing platform Nmi card vault is our choice tokenization vendor for data security. We chose them to take care of all of our card holder sensitive data storage, meaning we do not store any of this data ourselves.

6.3. CrossRiver Bank

https://crossriver.com
We use the Leading the Future of Finance | Cross River

Cross River is the trusted financial services organization that merges the established expertise of a bank, with the innovation and product offering of a technology company

6.4. Marqeta

https://www.marqeta.com/
Modern Card Issuing and Payment Solutions
We use the instantly issue cards and process card payments with an open API platform.

6.5. Twilio

https://www.twilio.com/
Twilio Customer Engagement Platform is a single platform with flexible APIs for any channel, built-in intelligence, and global infrastructure to support you at scale. We use the 2FA with the Twillio API

6.6. Rakuten

https://www.rakuten.com/
We use the Rakuten API for spending Wishers money and getting the Cash Back via API

7. Key Management

Key access – Keys must be protected such that only authorized users and applications can access the keys. The keys used to encrypt data should not be stored on the same media as that data.

1. Whenever keys are stored either physically or logically in close proximity to the data that it is protecting, mitigating controls must be in place to ensure a compromise of the data does not happen. Such mitigating controls must include, but are not limited to, the encryption of the keys themselves.
2. DR testing – Routine testing of key recovery should be based on the DR/BC plan associated with the system.
3. Audit reporting requirements – Usage of keys must be logged to provide an audit trail.
4. Cryptoperiod of the key – The lifetime of the key must be commensurate with the strength of the key and the data classification of the data that the key is used to encrypt. It is Wishes responsibility to define and adhere to the cryptoperiod.
5. Key Lifecycle: The lifecycle of the key can be summarized as generation, distribution, storage, usage, restoration (if necessary), and termination.

8. Incident Response Management

To detect system ic incidents, the following systems and processes are currently used:

a. Reports are sent to the telegram group
b. An Incident page is created in Asana detailing the incident and the steps to successfully mitigate it.

These methods are the entry points of every incident and cover any anomalies that are presented to the system for the main layers of our environment.

The incident response team is composed by the team members that have access to the Services Network, as described on item 5 - Personnel Responsibilities.

8.1. Incident Monitoring

At present, all events detected by the systems and processes above are forwarded to the engineering team through our telegram bot, which forwards the incidents to the engineering and infrastructure teams. This makes it possible to receive alerts of the production systems during the working team time (Monday - Friday 4 AM - 12 PM EST). Every Team Leader is responsible for monitoring these errors and forwarding, calling and letting the security team know in a timely fashion when an incident occurs.

For application-level incidents, we're able to post that to the Telegram channel, our main communication channel, for faster response and resolution times.

A couple hard requirements on our monitoring policy are:

a. All monitoring solutions used for perimeter protection and incident response generate logs;
b. The logs are stored by NGINx and MogoDB and saved for 60 days ;
c. Proxmox Backup Server performs daily backups and stores within Hetzner infrastructure.
d. The logs are stored on a server where only authorized personnel have access, to prevent that no modifications, damages for improper access is made to the log data;
e. The logs are stored for a period of 2 months are accessible to incident monitoring;

And once a real anomaly is identified, this is actually moved to the incident response process, which is described below.

8.2. Incident Response

Once an incident is detected, we move to the response process, which consists first of analyzing all of the incident data.

8.2.1. Identify the entry point

Once the incident event is dispatched, we know an approximate date/time that it happened given we enforce time integrity on our servers and applications through NTP. Through that, we're able to get a range of time which supposedly is when the event started and start detecting what was the entry point for that incident: is it an exception triggered by a user? Is this an actual malicious attacker? How did this attacker gain control over our system s – is it an application layer attack or is it a network level attack?

8.2.2. Identify anomalies in devices and the network

After understanding the origin, we need to automatically start mapping the affected devices, and observe how that translates to which services are being affected. This helps isolate the perimeter which is not affected on the healthy network, from the affected devices. Once that's detected, the server is isolated and the next part is actually inform ing our users and

customers of the incident;

8.2.3. Communicate the incident to the public

As we understand what is the scope of the incident, the first effort is categorizing its criticality and severity, to properly communicate to the public what is both our current status, and a plan of action to mitigate the issue. The four criticality types are:

a. Degraded Performance: when the incident just impacts the performance of our services, without further impact of outage;

b. Partial outage: when we understand that the incident is causing the services to be unstable, but for the majority of the time, they are operating or suffer degraded performance. Main triggers for this type of criticality are bound to geolocation, connection type, volume being processed, and other variable criteria;

c. Major outage: when we understand that the services are unstable for the majority of the time, or fully unavailable. These outages can be considered actual downtime;

d. Under maintenance: when we're either under a scheduled maintenance, or under emergency maintenance, which causes the system to be fully unavailable.
Once the incident response team fully categorizes the incident, we move to the actual communication phase which consists of creating a new incident.

All of that is organized through the communication inside the DevOps and Development team. This helps keeping communication consistent, and prevents misleading information to be posted on different channels.

8.2.4. Mitigate the incident and handle its constant update

After issuing clear communications to the relevant parties, we involve the other areas of the company to mitigate the incident, which would consist in the communication inside the DevOps and Development team:

a. Engineering team, and the task should be created as a Support Request;

b. Infrastructure & DevOps team and the task should be created as an Infrastructure Change Request;

9. Clear Desk Policy

1. Employees are required to secure all sensitive/confidential information in their workspace at the conclusion of the work day and when they are expected to be away from their workspace for an extended period of time. This includes both electronic and physical hardcopy information.
2. Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the work day. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.

3. Printed materials must be immediately removed from printers or fax machines. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible.
4. All sensitive documents and restricted information must be placed in the designated shredder bins for destruction, or placed in the locked confidential disposal bins. Please refer to the Records Retention Policy for additional information pertaining to document destruction.
5. File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.
6. Passwords must not be written down or stored anywhere in the office.

10. Data and Logs Storage

Our environment keeps the middle-level standards of security for storage and is backed up, by relying on both our own technology and on Hetzner expertise to run backups and make sure our data is always restorable with as minimal impact as possible.

10.1. Log Management and Backups

Our environment is based on .

- Daily Database and media backups
- NGINX logs
- MongoDB logs
- Ping based website monitoring
- SSL monitoring

All of this is provided by Proxmox Backup Server

10.2. Database Backups

We use the Proxmox Backup Server which means it is backed up daily and stored within Hetzner infrastructure.

11. Removable Media / Storage Device Policy

Removable media takes many forms today (jump drives, flash memory storage, portable storage devices, etc.). Removable media is personal, removable, and portable which introduces risk into the organization whenever it is used to store sensitive information. Aside from the chance for loss and theft, removable media format storage is a well-known source of malware infections and has been directly tied to the loss of information.

Removable media storage of any type shall generally be disallowed in any form or function within the Wishes operational environment. Personal storage devices shall not be used for storage of any Wishes information or be used with Wishes hardware. Exceptions to this policy

shall be considered only in unique and rare cases. These requests shall require written approval of the CEO and be granted only for justifiable business purposes.