TERM PROJECT

Information Security Policy

Document

Group 4	
Syeda Maham Jafri	22796
Maaz Siddique	22997
Ashnah Khalid Khan	22889
Zohaib Azam	22732
Syed, Danial Haseeb	

Contents

1 Acknowledgments

The following document was largely developed using policy guidelines, templates and requirements publicly available on the SANS Institute for cybersecurity training and the Ministry of Information Technology & Telecommunication of the Government of Pakistan.

2 Introduction

A comprehensive information security policy is essential for any organization to protect information assets and ensure data integrity, confidentiality, and availability. This document presents an Information Security Policy for "Jetzy". Recognizing the unique security needs of the industrial sector, this policy establishes robust measures to guard against threats and vulnerabilities. Jetzy aims to enhance its security posture, comply with industry standards and regulations, and foster a culture of security awareness among employees, partners, and users. The policy includes detailed procedures and controls for data protection, access management, and incident response, tailored to Jetzy's needs, along with a step-by-step implementation plan.

2.1 Organization Overview

Company Profile

Jetzy is a leading social media application designed for travelers. It connects users, enabling them to share experiences, find and book hotels, make restaurant reservations, and enjoy various travel-related services. With a focus on creating a seamless travel experience, Jetzy provides users with the tools they need to plan and share their journeys. The company offers its services as a website, as well as an iOS and Android mobile app.

Key Services

Jetzy offers a range of services designed to enhance the travel experience for its users, including:

- Post uploading and sharing
- User groups and messaging
- Hotel booking
- Restaurant reservations
- Paid membership features

Contact Information

For any inquiries or support, please contact Jetzy at:

- **Address:** 205 E 42nd, 16th Floor, New York, NY 10017
- **Email:** contact@jetzy.com / shamazehra@jetzyapp.com (CEO of Jetzy)
- **Phone:** +1 (734) 330-0575

Current Information Security Scope & Boundaries

Jetzy's information security scope encompasses both internal and external factors affecting the organization's security posture. Key focus areas include:

- Protection of user data and privacy.
- Securing the infrastructure of the platform, covering both the website and mobile app.
- Ensuring compliance with relevant industry standards and regulations.
- Managing risks associated with third-party services and integrations.
- Implementing robust incident response and disaster recovery plans.

However, several shortcomings have been identified:

- Remote employee usage has not been addressed adequately.
- Weak physical security measures are in place on-premise, lacking screening for Jetzy-issued and Jetzy-verified devices.
- DevSecOps or secure development techniques are not integrated into current practices.
- Employees lack awareness regarding security protocols, data classification, and incident response procedures.
- There are no regulations governing the secure usage of communication systems.
- The organization lacks an Enterprise-level Intrusion Detection and Prevention System (IDPS).
- The security infrastructure is not built upon a Public-key Infrastructure (PKI).

Addressing these shortcomings will be paramount to enhancing Jetzy's overall information security posture.

2.2 Vision

Jetzy's information security vision is:

To be the global lead in social networking platforms that fosters an ethical, safe and trustworthy digital environment for all, by leveraging advanced and robust technologies to protect the privacy and integrity of our organization and our users' data from ever-evolving information security threats. To develop a seamlessly secure, reliable, and innovative app that is every person's first choice for embarking on their travel experience.

2.3 Statement of Purpose

The purpose of this Information Security Policy is to establish a framework to safeguard Jetzy's information assets, ensuring the confidentiality, integrity, and availability of data. This policy outlines the strategic and procedural measures necessary to protect our social media platform's infrastructure, user data, and business operations from potential security threats and vulnerabilities.

Recognizing the critical importance of information security in the digital age, Jetzy is committed to implementing robust security practices that comply with industry standards and regulations. This policy aims to foster a culture of security awareness among employees, partners, and users, while promoting the use of advanced technologies to mitigate risks.

By adhering to this policy, Jetzy seeks to enhance its security posture, protect sensitive information, and maintain the trust and confidence of its users and stakeholders. The policy includes comprehensive guidelines for data protection, access management, incident response, and continuous improvement, tailored to meet the unique needs of our organization.

Ultimately, this Information Security Policy serves as a cornerstone of Jetzy's commitment to providing a secure, reliable, and innovative platform for travelers worldwide.

2.4 Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals or organizations that interact with Jetzy's information systems and data. It ensures comprehensive protection and governance over all physical and virtual aspects of Jetzy's operations, including but not limited to:

- Protection of physical assets, including offices, data centers, and equipment.

- Measures to protect the integrity and privacy of network communications and infrastructure.
- Policies and procedures related to employee and contractor access, roles, and responsibilities.
- All physical devices involved in accessing, processing, or storing Jetzy's data.
- Applications and systems used within Jetzy, including both proprietary and third-party software.
- External services and platforms used by Jetzy, including cloud services and external vendors.
- User interface and user experience technologies, primarily Flutter.
- Server-side technologies and frameworks, specifically Elixir.
- Source code and version management systems, including Git.
- Services and platforms provided by Google Cloud Platform, encompassing computing, storage, and networking services.
- Internal and external communication technologies, such as email systems and messaging platforms.
- Tools and technologies for protecting information assets, including firewalls, encryption tools, anti-malware software, and intrusion detection/prevention systems.

2.5 Objectives

By developing and implementing this information security policy, the organization aims to meet the following objectives:

- Ensure compliance with pertinent laws, regulations, and industry standards governing information security practices.
- Foster a culture of cybersecurity awareness among Jetzy's employees, partners, and users through comprehensive education, training, and communication initiatives.
- Implement a security-first approach to the development process and incorporate DevSecOps practices throughout the organization.
- Strengthen existing security measures to guarantee that only authenticated and authorized individuals access Jetzy's data and information assets, thereby preserving confidentiality.

- Integrate frameworks for regulation, assurance, threat management, and incident response to effectively manage risks and policy violations.
- Preserve the integrity of Jetzy's data and IT systems, ensuring that information remains intact, accurate, and complete.
- Ensure the uninterrupted operation of Jetzy's systems and services, even during security incidents or disruptions, by developing extensive incident response, disaster recovery, and business continuity plans and measures.
- Establish an information assurance framework for continuous monitoring, logging, and auditing to ensure compliance with cybersecurity standards across Jetzy and its partners.

3 Definitions & Terms

3.1 Definitions

- **Personally Identifiable Information (PII):** Information that can be used to identify, contact, or locate a single person, or to identify an individual in context. Examples include names, addresses, phone numbers, and social security numbers.
- **Chief Information Security Officer (CISO):** The executive responsible for an organization's information and data security.
- **Operational Security (OPSEC):** A process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.
- **Information Security (INFOSEC):** The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information.
- **Communication Security (COMSEC):** Measures taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such communications.
- **Development, Security, and Operations (DevSecOps):** A software development methodology that integrates security practices within the DevOps process.
- **End-to-End Encryption (E2EE):** A method of secure communication that prevents third parties from accessing data while it's transferred from one end system or device to another.
- **Command Injection:** An attack technique in which the goal is to execute arbitrary commands on the host operating system via a vulnerable application.
- **Cross-site Scripting (XSS):** A security vulnerability typically found in web applications which allows attackers to inject client-side scripts into web pages viewed by other users.
- **SQL Injection:** A code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques.

- **Globally Unique Identifier (GUID):** A unique reference number used as an identifier in software.
- **Air-gapped Environment:** A network security measure employed to ensure that a computer or network is physically isolated from unsecured networks.
- **Data-at-rest:** Inactive data that is stored physically in any digital form (e.g., databases, data warehouses, spreadsheets, archives, tapes, off-site backups).
- **Data-in-transit:** Data actively moving from one location to another such as across the internet or through a private network.
- **Network Segmentation:** The process of dividing a network into multiple segments or subnets, each acting as its own small network, to improve security and performance.
- **Patch Management:** The process of distributing and applying updates to software.
- **Separation of Duties (SoD):** A security principle aimed at preventing fraud and error by ensuring that no single individual has control over all phases of a transaction.
- **Least Privilege:** The practice of limiting access rights for users to the bare minimum permissions they need to perform their work.
- **Redundancy:** The duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe.
- **Load Balancing:** A technique used to distribute workloads uniformly across multiple servers or other resources to optimize resource use, reduce latency, and ensure high availability.
- **Six E's:** A security concept focusing on different areas such as Engagement, Empowerment, Education, Enablement, Enforcement, and Endurance to enhance security posture.

4 Modification & Revision

- This policy will be reviewed at least bi-annually.
- In addition, this policy can be reviewed and modified as and when necessary.

5 Roles & Responsibilities

6 Roles & Responsibilities

6.1 Chief Executive Officer (CEO)

- The CEO holds ultimate responsibility for ensuring that the organization's information security strategy aligns with its business objectives and regulatory requirements.
- Approves the information security policy and ensures adequate resources are allocated for its implementation.
- Ensures the organization's leadership fosters a culture of security awareness and compliance.

6.2 Chief Information Security Officer (CISO)

- Overall responsibility for the development, implementation, and management of the organization's information security policies and practices.
- Oversees risk management, incident response, and compliance with legal and regulatory requirements.
- Reports to the CEO and the board of directors on the state of the organization's information security posture.

6.3 Chief Information Officer (CIO)

- Collaborates with the CISO to ensure that information security is integrated into the organization's IT strategy.
- Manages the IT infrastructure and ensures that security controls are implemented and maintained.
- Ensures that the IT team is trained and aware of their responsibilities regarding information security.

6.4 Data Protection Officer (DPO)

- Ensures compliance with data protection regulations such as GDPR and CCPA.

- Manages data subject requests and handles data breach notifications.
- Provides guidance on data protection impact assessments and privacy by design principles.

6.5 IT Security Team

- Implements security measures, monitors security systems, and responds to security incidents.
- Ensures that the security policies are followed and provides support and guidance on security matters.
- Conducts regular security assessments and vulnerability testing.

6.6 Compliance Officer

- Ensures that the organization complies with all relevant laws, regulations, and industry standards.
- Conducts regular audits and assessments to ensure compliance.
- Works with the IT Security Team to address compliance-related issues and implement necessary changes.

6.7 Developers and Engineers

- Adhere to secure coding practices and integrate security into the development lifecycle.
- Ensure that their work complies with the organization's security policies and standards.
- Participate in security training and awareness programs.

6.8 All Employees

- Follow security policies and procedures, and report security incidents or suspicious activities.
- Participate in security training and awareness programs to stay informed about security best practices and threats.
- Ensure the secure use of organizational resources and protect sensitive information.

6.9 Third-Party Vendors

- Comply with Jetzy's security requirements and ensure their own security measures are adequate to protect any shared data.
- Undergo security assessments before being granted access to Jetzy's network or data.
- Cooperate with Jetzy's compliance and security policies and participate in regular security reviews and audits.

7 Physical Security Policy

7.1 Physical Access Controls

1. Employees are only allowed to used Jetzy-issued devices including laptops, USBs, microphones/headphones, mice, keyboards, monitors etc to access Jetzy systems, servers, platforms and tools. Any other devices must not be allowed connection to these platforms under any circumstances.

2. Remote employees will only be allowed access to Jetzy systems, servers, platforms and tools once they have been handed over a Jetzy-issued device for their work, or their existing device is configured to connect to Jetzy after clearing all necessary security checks and requirements.

3. For the purpose of this section, the term "Jetzy devices" will be used to refer to all Jetzy-issued and Jetzy-verified devices used by both remote and physical employees of the organization.

4. All Jetzy devices must at least be configured with the following hardware requirements: a biometric authentication device, Key Card reader to authenticate the unique Key Card issued to employees of the organization, explicit webcam control and microphone control features.

5. All Jetzy devices must at least be configured with the following software requirements: a Linux operating system, Outlook and relevant email scanning extensions, company-wide used antivirus and anti-malware software, firewalls, organization-approved VPN, and relevant protocols for secure email, internet, wireless and web transactional use as outlined in this document.

6. Employees are not permitted to remove these devices from their work stations or take them home unless these instances are recorded.

7. The organization must maintain measures to automically log relevant details related to devices being removed and returned to their workstations. This must include information that will help identify the device, the time, location, individual performing the act etc.

8. All physical asset locations including DMZs will be separated by gates requiring MFA, including bio-metric authentication and automatic ID card verification, for entrance of only permitted individuals authorized to access those areas.

9. All departments and areas will be allowed to be accessed only by the employees and staff authorized to access that area, and all entrance and exiting of individuals recorded and logged with their relevant details.

10. CCTV surveillance will be installed organization-wide and reviewed and audited weekly by the security team.

11. Five failed login/access attempts at any non-critical physical facility at the organization will immediately trigger an alert and the corresponding incident response plan will be initiated to deal with the issue accordingly.

12. Three failed login/access attempts at any critical physical facility at the organization will immediately trigger an alert and the corresponding incident response plan will be initiated to deal with the issue accordingly.

13. Five failed virtual login/access attempts to any system, network, server, platform or device at the organization will immediately trigger an alert and the corresponding incident response plan will be initiated to deal with the issue accordingly.

14. Intrusion detection alarms will be installed and sounded once the limit for failed access attempts is crossed or on unauthorized access to the respective areas in the organization, and respective security personnel notified.

15. The organization will contain multiple air gap environments to scan any external physical devices before they are authorized to connect the main organization networks and devices to avoid worms and lessen the likelihood of RCE attacks.

7.2 Demilitarized Zones

1. All equipment owned and/or operated by Jetzy located outside Jetzy's corporate Internet firewalls, including devices facing the Internet and beyond Jetzy's firewall, constituting the "de-militarized zone" (DMZ), must strictly adhere to the standards defined in this policy due to their vulnerability to Internet attacks.

2. This policy applies to all equipment deployed in a DMZ owned and/or operated by Jetzy, including hosts, routers, switches, etc.

3. Support groups approved by Infosec for DMZ system, application, and/or network management must administer equipment within the scope of this policy, documenting equipment in the corporate-wide enterprise management system, maintaining network interfaces, managing password groups, granting immediate access to equipment and system logs to Infosec, and ensuring compliance with change management processes.

4. Infosec will periodically audit DMZ equipment to verify compliance with this policy, including hardware, operating systems, services, and applications receiving approval from Infosec, installation of all patches/hot-fixes

recommended by the equipment vendor and Infosec, and replacement of insecure services or protocols with more secure equivalents.

5. Trust relationships between systems must be documented and approved by Infosec, and remote administration must occur over secure channels or console access independent from the DMZ networks, with security-related events logged and audit trails saved to Infosec-approved logs, and non-compliance waiver requests addressed by Infosec on a case-by-case basis.

6. All new installations and changes to existing equipment and applications must adhere to the DMZ Equipment Deployment Process and Corporate Change Management Procedures, with Infosec invited to perform system/application audits before the deployment of new services, and all new deployments and configuration changes receiving approval from Infosec.

7. The responsibility for the security of equipment deployed by external service providers must be clarified in contracts, with security contacts and escalation procedures documented, and contracting departments ensuring third-party compliance with this policy.

8. All networks and equipment deployed in Jetzy labs situated on the "De-Militarized Zone" (DMZ) must strictly adhere to the information security requirements outlined in this policy, including those in primary Internet Service Provider (ISP) locations and remote areas.

9. Business justification for all new DMZ Labs must be provided and signed off at the business unit Vice President level, with records maintained by the Infosec Team, and lab owning organizations designating lab managers and points of contact (POC), maintaining up-to-date information with the Infosec Team, and ensuring availability around-the-clock for emergencies.

10. Changes to existing DMZ Labs and establishment of new ones require approval from the Infosec Team after a request through Jetzy Network Support Organization, with maintenance of ISP connections and firewall devices between DMZ Labs and the Internet the responsibility of Jetzy Network Support Organization, and the Infosec Team and Network Support Organization reserving the right to interrupt lab connections if security concerns arise.

11. DMZ Lab managers are required to provide and maintain network devices up to the Network Support Organization point of demarcation, with the Network Support Organization recording all DMZ Lab address spaces and contact information, and DMZ Lab Managers holding ultimate responsibility for ensuring compliance with this policy.

12. Members of the Infosec Team and Network Support Organization must have immediate access to equipment and system logs upon request, following the Audit Policy, with individual lab accounts deleted within three (3) days of access termination, and group account passwords changed within the same timeframe of group membership changes, and non-compliance waiver requests reviewed and addressed by the Infosec Team on a case-by-case basis.

13. DMZ Labs must not establish direct or wireless connections to Jetzy's corporate internal networks and should be physically separate or in locked racks with limited access, with Lab Managers responsible for ensuring compliance with the Password Policy, Wireless Communications Policy, and Lab Policy, and firewall devices maintained by the Network Support Organization strictly adhering to least-access principles and DMZ Lab business needs, with configurations reviewed and approved by the Infosec Team.

14. Traffic between DMZ Labs and the Jetzy internal network, including VPN access, falls under the jurisdiction of the Remote Access Policy, with routers and switches not designated for testing/training purposes conforming to DMZ Router and Switch standardization documents, and hosts running Internet Services in DMZ Lab strictly adhering to secure installation and configuration standards, with up-to-date security patches/hot-fixes applied and services and applications not serving business requirements disabled.

15. Jetzy Confidential information is strictly prohibited in labs with non-Jetzy personnel physical access, in accordance with the Data Classification and Protection Policy, and remote administration must occur exclusively over secure channels or through independent console access from DMZ networks.

7.3 Information & Equipment Disposal

1. All technology equipment and components owned by Jetzy must undergo proper disposal procedures upon reaching the end of their useful life.

2. This policy applies to all computer/technology equipment or peripheral devices that are no longer required within Jetzy, encompassing personal computers, servers, hard drives, laptops, smartphones, peripherals, printers, scanners, compact and floppy discs, portable storage devices, backup tapes, and printed materials.

3. When technology assets have fulfilled their usefulness, they must be promptly forwarded to the ¡Equipment Disposal Team¿ office for appropriate disposal.

4. The ¡Equipment Disposal Team¿ is obligated to securely erase all storage media using industry best practices.

5. All data, including files and licensed software, must be eliminated from equipment using disk sanitizing software meeting Department of Defense standards, ensuring the overwriting of each disk sector with zero-filled blocks.

6. Under no circumstances may computer or technology equipment be sold to individuals outside of the procedures outlined in this policy.

7. Disposal of computer equipment via skips, dumps, or landfills is strictly prohibited; electronic recycling bins provided by Jetzy should be utilized for proper equipment disposal.

8. Electronic drives must undergo degaussing or be overwritten with a commercially available disk cleaning program; hard drives may also be physically destroyed through methods such as drilling or crushing.

9. The ¡Equipment Disposal Team¿ is required to affix a sticker on the equipment case post-disk wipe, indicating the date and initials of the technician who performed the operation.

10. Technology equipment with malfunctioning memory or storage technology must have the memory/storage device removed and physically destroyed.

11. Working equipment that has reached the end of its useful life at Jetzy will be made available for purchase by employees through a lottery system.

12. All equipment purchases must follow the lottery process to ensure fair distribution among employees; direct purchase or reservation of systems is prohibited.

13. The Finance and Information Technology departments will determine the appropriate cost for each item, and all purchases are final, with no warranty or support provided.

14. Any equipment remaining from the lottery process or not in working order will be either donated or disposed of according to current environmental guidelines.

15. Before leaving Jetzy premises, all equipment must be removed from the Information Technology inventory system.

16. Physical copies of data, e.g from photocopies, scanners and printers, should be safely disposed to safeguard the unauthorized access of sensitive data.

17. Jetzy devices returned by former employees must be digitally cleaned, screened and reconfigured to extract and store any sensitive information already contained in the device if needed, before it is assigned to a new owner to avoid its unauthorized use by the new owner.

8 Network Security

8.1 Networks

1. All organization networks must adhere to the relevant standards and compliance laws detailed in this document.
2. Network segmentation must be implemented extensively throughout the organization to segregate external, internal, sensitive, and highly sensitive networks based on roles, separation of duties, departments, access etc accordingly.
3. All connections made to the organizational network must be done from VPN-configured devices, that must contain firewalls and organization-enforced NIDPS tools.

8.2 Remote Access

1. Remote access to the organization's networks must be done only from Jetzy-issued or Jetzy-verified devices.
2. All other requirements for on-premises network connections apply to remote access as well.

8.3 Server

1. Each operational group at Jetzy must own internal servers deployed for system administration. They are required to establish and maintain approved server configuration guides, monitor compliance, and adhere to an exception policy approved by the InfoSec team.
2. Servers deployed within Jetzy must be registered in the corporate enterprise management system, ensuring updated information such as server contacts, location, hardware, operating system/version, and main functions/applications.
3. Any changes to production server configurations must follow appropriate change management procedures.
4. Authorized personnel have the responsibility to monitor and audit equipment, systems, processes, and network traffic for security, compliance, and maintenance purposes in accordance with the Audit Policy.
5. Operating system configurations must adhere to approved guidelines provided by the InfoSec team.

6. Unused services and applications must be disabled, and access to services should be logged or protected through access control methods.

7. All servers must have the most recent security patches installed promptly, except when immediate application would disrupt business operations.

8. Trust relationships between systems should be avoided unless absolutely necessary, and standard security principles of least required access must be implemented.

9. Privileged access should be conducted over secure channels where available, and servers must be physically located in access-controlled, secured environments.

10. Servers are strictly prohibited from operating in uncontrolled or unsecured cubicle areas.

11. Security-related events on critical or sensitive systems must be logged, with audit trails retained online for a minimum of one week, daily incremental tape backups retained for at least one month, weekly full tape backups of logs retained for at least one month, and monthly full backups retained for a minimum of two years.

12. InfoSec must be notified of security-related events for review, with incidents reported to IT management, and appropriate corrective measures taken. These events include port-scan attacks, unauthorized access to privileged accounts, and anomalous occurrences unrelated to specific applications on the host.

8.4 Internet DMZ Equipment

1. All equipment owned and/or operated by Jetzy located outside Jetzy's corporate Internet firewalls must strictly adhere to the standards defined in this policy.

2. Devices facing the Internet and beyond Jetzy's firewall, constituting the "de-militarized zone" (DMZ), are subject to this policy due to their vulnerability to Internet attacks.

3. All equipment deployed in a DMZ owned and/or operated by Jetzy, including hosts, routers, switches, etc., must comply with this policy.

4. Support groups approved by Infosec for DMZ system, application, and/or network management must administer equipment within the scope of this policy.

5. Support groups are required to document equipment in the corporate-wide enterprise management system, maintain network interfaces, manage password groups, grant immediate access to equipment and system logs to Infosec, and ensure compliance with change management processes.

6. Infosec will periodically audit DMZ equipment to verify compliance with this policy.

7. Hardware, operating systems, services, and applications must receive approval from Infosec, and operating system configuration must adhere to secure host and router installation and configuration standards.

8. All patches/hot-fixes recommended by the equipment vendor and Infosec must be installed, and services and applications not serving business requirements must be disabled.

9. Trust relationships between systems must be documented and approved by Infosec, and insecure services or protocols must be replaced with more secure equivalents.

10. Remote administration must occur over secure channels or console access independent from the DMZ networks, and all host content updates must occur over secure channels.

11. Security-related events must be logged, and audit trails saved to Infosec-approved logs; non-compliance waiver requests will be addressed by Infosec on a case-by-case basis.

12. All new installations and changes to existing equipment and applications must adhere to the DMZ Equipment Deployment Process and Corporate Change Management Procedures.

13. Infosec must be invited to perform system/application audits before the deployment of new services, and all new deployments and configuration changes must receive approval from Infosec.

14. The responsibility for the security of equipment deployed by external service providers must be clarified in contracts, with security contacts and escalation procedures documented, and contracting departments must ensure third-party compliance with this policy.

8.5 DMZ Lab Security

1. All networks and equipment deployed in Jetzy labs situated on the "De-Militarized Zone" (DMZ) must strictly adhere to the information security requirements outlined in this policy.

2. The policy applies to DMZ Labs located outside Jetzy corporate Internet firewalls, including those in primary Internet Service Provider (ISP) locations and remote areas.

3. Business justification for all new DMZ Labs must be provided and signed off at the business unit Vice President level, with records maintained by the Infosec Team.

4. Lab owning organizations must designate lab managers and points of contact (POC), maintain up-to-date information with the Infosec Team, and ensure availability around-the-clock for emergencies.

5. Changes to existing DMZ Labs and establishment of new ones require approval from the Infosec Team after a request through Jetzy Network Support Organization.

6. Maintenance of ISP connections and firewall devices between DMZ Labs and the Internet is the responsibility of Jetzy Network Support Organization.

7. The Infosec Team and Network Support Organization reserve the right to interrupt lab connections if security concerns arise.

8. DMZ Lab managers are required to provide and maintain network devices up to the Network Support Organization point of demarcation.

9. The Network Support Organization must record all DMZ Lab address spaces and contact information.

10. DMZ Lab Managers hold ultimate responsibility for ensuring compliance with this policy.

11. Members of the Infosec Team and Network Support Organization must have immediate access to equipment and system logs upon request, following the Audit Policy.

12. Individual lab accounts must be deleted within three (3) days of access termination, and group account passwords changed within the same timeframe of group membership changes.

13. Non-compliance waiver requests will be reviewed and addressed by the Infosec Team on a case-by-case basis.

14. DMZ Labs must not establish direct or wireless connections to Jetzy's corporate internal networks and should be physically separate or in locked racks with limited access.

15. Lab Managers are responsible for ensuring compliance with the Password Policy, Wireless Communications Policy, and Lab Policy.

16. Firewall devices maintained by the Network Support Organization must adhere strictly to least-access principles and DMZ Lab business needs, with configurations reviewed and approved by the Infosec Team.

17. Traffic between DMZ Labs and the Jetzy internal network, including VPN access, falls under the jurisdiction of the Remote Access Policy.

18. Routers and switches not designated for testing/training purposes must conform to DMZ Router and Switch standardization documents.

19. Hosts running Internet Services in DMZ Lab must strictly adhere to secure installation and configuration standards, with up-to-date security patches/hot-fixes applied.

20. Services and applications not serving business requirements must be disabled.

21. Jetzy Confidential information is strictly prohibited in labs with non-Jetzy personnel physical access, in accordance with the Data Classification and Protection Policy.

22. Remote administration must occur exclusively over secure channels or through independent console access from DMZ networks.

9 Communications security

9.1 Email

1. This policy is established to mandate the appropriate utilization of the Jetzy Outlook email system, defining acceptable and unacceptable practices in electronic communications.

2. All users of the Jetzy Outlook email system, including employees, vendors, and agents acting on behalf of Jetzy, are required to adhere to this policy.

3. Email usage within Jetzy must align with the organization's policies, ethical standards, safety protocols, legal requirements, and established business practices without exception.

4. Users must refrain from creating or disseminating disruptive or offensive messages through the Jetzy Outlook email system. Offensive content based on attributes such as race, gender, religion, etc., must be reported promptly to the supervisor.

5. Jetzy Outlook email accounts are designated primarily for business-related purposes. Limited personal communication is permitted, with non-Jetzy related commercial activities strictly prohibited.

6. All Jetzy data within email messages or attachments must be safeguarded according to the Data Protection Standard without compromise.

7. All email correspondence within Jetzy Outlook must fully comply with the encryption, digital certificate, and digital signature requirements specified in this policy, with no exceptions.

8. Automatic forwarding of Jetzy Outlook email to third-party email systems is strictly prohibited. Forwarded messages must not contain Jetzy confidential or sensitive information.

9. Users are strictly prohibited from conducting Jetzy business, executing binding transactions, or storing Jetzy Outlook email on external email systems or storage servers under any circumstances.

10. Jetzy employees must acknowledge and accept that they have no expectation of privacy regarding any content stored, sent, or received via the company's Outlook email system.

11. Employees must exercise utmost caution when providing sensitive information via email within Jetzy Outlook, ensuring they authenticate the recipient's identity and validate the legitimacy of the request.

12. For emails involving actionable operations, processes, or directives, the Maker-Checker or 6-Eyes principle must be rigorously implemented within Jetzy Outlook to verify the authorization of the action, the identity of the sender, and the involvement of the relevant subject.

13. Jetzy reserves the right to monitor email messages within Jetzy Outlook without prior notice, although such monitoring is discretionary and not obligatory.

14. Users within Jetzy Outlook are mandated to undergo regular training on identifying and avoiding phishing attempts. Immediate reporting of any suspicious emails to the IT department is imperative.

15. Before opening or clicking on email attachments and links within Jetzy Outlook, users are required to conduct thorough scanning for malware and other threats to prevent security breaches.

16. All email threats and malware scanning tools must be up-to-date at all times.

17. Jetzy's Outlook email system may employ scanning mechanisms to detect and prevent phishing attempts, malware, and other cyber threats. Users within Jetzy Outlook must fully cooperate with these security measures and promptly report any anomalies or suspected security breaches.

9.2 Internet Usage

1. The IT department will generate and assign internet credentials, including usernames and passwords, upon approval of users' internet access requests.

2. Internet credentials will be revoked upon termination of employment, completion of service, or disciplinary action, adhering to the organization's access control policies.

3. Default internet credentials will be reset upon initial assignment to ensure security. Users must change their default passwords within [specific time period] of receiving their credentials.

4. Temporary or contractual employees will receive temporary internet credentials for the duration of their employment or contract, revoked upon termination or completion of service.

5. Management will oversee the assignment and revocation of temporary internet credentials, ensuring compliance with access control policies and timely removal of access.

6. Internet access is solely granted to support business activities necessary for job functions.

7. All Jetzy network users, including employees, vendors, and agents, must comply with the Internet Usage Policy and associated Internet/Intranet Security Policy.

8. Internet access is provided based on reasonable business needs identified in users' current job responsibilities.

9. Users must read and sign both the Internet Usage Policy and associated Internet/Intranet Security Policy acknowledgment forms before access is granted.

10. Internet access requests, accompanied by a signed Internet Usage Coverage Acknowledgment Form, must be submitted to the IT department.

11. Internet access will cease upon termination of employment or contract, completion of service, or disciplinary action for policy violation.

12. Inactive user IDs will be revoked after thirty (30) days, with access privileges reevaluated annually by management.

13. Internet usage must be for business purposes only, with users exercising good judgment in resource usage.

14. Users must comply with corporate principles regarding resource usage, refraining from unauthorized activities such as gambling, unauthorized downloading, gaming, or online contest participation.

15. All internet activities are subject to monitoring, with users aware of the audit log reflecting service requests and periodic reviews.

16. Users must not transmit personal information without proper controls, and unauthorized access to sensitive data is strictly prohibited.

17. The company prohibits illegal, offensive, libelous, threatening, harassing, or discriminatory conduct, fraudulent activities, or dissemination of false materials.

18. Users must adhere to bandwidth guidelines, avoiding negatively impacting other employees' internet usage.

19. Software copying and material reproduction from the internet must comply with software vendors' license agreements and copyright laws.

20. Management reserves the right to examine email, personal file directories, web access, and stored information without notice to ensure policy compliance.

21. Users should not assume email communication is confidential, aware that electronic communications can be forwarded, intercepted, printed, and stored by others.

22. When representing the company online, users must clearly indicate their opinions are their own and not necessarily those of the company.

23. Users are prohibited from posting company material on public forums without proper authorization from management and the public relations department.

24. Establishment of company web pages requires formal authorization and compliance with IT department standards.

25. All company web sites must be protected from intrusion through formal security measures provided by the IT department.

26. Periodic reviews will ensure compliance with usage policies, with modifications based on company information needs.

9.3 Wireless Communication

1. Wireless infrastructure devices connecting to the Jetzy network must meet the standards outlined in this policy or receive an exception granted by the Information Security Department.

2. All personnel, including employees, contractors, consultants, temporary workers, and third-party individuals managing wireless infrastructure devices on behalf of Jetzy, are required to comply with this policy.

3. Devices granting access to Jetzy Confidential or higher information must adhere to the standards specified in the Wireless Communication Standard.

4. These devices must be installed, supported, and maintained by an approved support team, utilizing authentication and encryption protocols approved by Jetzy.

5. It is mandatory for these devices to possess a hardware address (MAC address) that can be registered and tracked, while refraining from disrupting wireless access deployments of other support organizations.

6. Lab wireless devices providing access to Jetzy Confidential or higher information must conform to the aforementioned standards and be isolated from the corporate network in accordance with the Lab Security Policy.

7. Home wireless devices enabling direct access to the Jetzy corporate network must adhere to the Home Wireless Device Requirements delineated in the Wireless Communication Standard.

8. Devices failing to meet these standards must be configured to prevent direct access to the corporate network, permitting access only through standard remote authentication methods.

9. All network devices must be procured, supported, and managed by an Information Security approved support organization, following the Lab Security Policy guidelines for lab devices.

10. Every individual associated with Jetzy, including employees, contractors, consultants, and temporary workers, is obligated to uphold these standards, including those responsible for managing wireless infrastructure devices.

11. Any deviations from these standards necessitate prior approval from the Information Security (InfoSec) Team.

12. Devices establishing connections to the Jetzy network or granting access to sensitive data must utilize designated authentication protocols and encryption methodologies.

13. Bluetooth devices must implement Secure Simple Pairing with encryption activated.

14. Lab device SSID must be distinct from the production device SSID, with the lab SSID broadcast turned off.

15. Home wireless devices must employ WPA-PSK, EAP-FAST, PEAP, or EAP-TLS, with intricate shared secret keys for WPA-PSK, SSID broadcast disabled, default SSID name altered, and default login/password adjusted.

9.4 Remote Access

1. Remote access to the corporate network must strictly adhere to encryption protocols such as Virtual Private Networks (VPNs) and robust passphrases, as detailed in the Acceptable Encryption Policy and the Password Policy.

2. Authorized Users are required to diligently safeguard their login credentials and passwords, refraining from any sharing, even with family members.

3. While remotely connecting to Jetzy's corporate network using a Jetzy-owned computer, Authorized Users must ensure that the remote host is exclusively connected to Jetzy's network, except for personal networks under their complete control or that of an Authorized User or Third Party.

4. External resources utilized for Jetzy business purposes must undergo prior approval from InfoSec and the respective business unit manager.

5. All hosts connecting to Jetzy's internal networks via remote access technologies must utilize the most recent anti-virus software, including personal computers, in accordance with the Hardware and Software Configuration Standards for Remote Access to Jetzy Networks.

6. Only remote access tools that have been approved, monitored, and appropriately controlled may be utilized on Jetzy computer systems to mitigate the risk of unauthorized access or asset damage.

7. All remote access tools facilitating communication with Jetzy resources or external partner systems from the Internet must incorporate multi-factor authentication, such as authentication tokens or smart cards, requiring an additional PIN or password.

8. The authentication database source for remote access tools must be Active Directory or LDAP, utilizing a challenge-response protocol resilient to replay attacks, and must mutually authenticate both ends of the session.

9. Remote access tools must utilize the Jetzy application layer proxy instead of establishing direct connections through perimeter firewalls.

10. End-to-end encryption of remote access communication channels must align with Jetzy's network encryption protocols policy.

11. Jetzy's antivirus, data loss prevention, and other security systems must remain active and operational without any interruption or circumvention while remote access tools are in use.

12. All acquisitions of remote access tools must adhere to Jetzy's standard procurement process, requiring approval from the information technology group.

13. Remote access to the organization's network is exclusively permitted through devices issued by Jetzy and verified to have features that restrict access to authorized devices only.

10 Information Security Policy

10.1 Data Classification

1. The purpose of this data classification policy is to establish a framework for classifying Jetzy's data based on its sensitivity, value, and criticality to the organization. Proper data classification ensures that data is handled with appropriate security measures to protect confidentiality, integrity, and availability.

2. Organization resources, including hardware, devices, data, time, and software, must be classified based on their criticality and business value.

3. Jetzy must follow the NIST standards for organizational data classification.

4. Jetzy's data must be classified into three sensitivity levels: Low, Medium, and High, each corresponding to specific data types and security measures.

5. Low Sensitivity Data:

    a) Description: Data that would have minimal impact if compromised, intended for public use without confidentiality protections.

    b) Examples: Public information and web pages (e.g., job postings, blog posts), press releases, user location data etc.

    c) Security Measures: Data must be freely shared within and outside the organization. Basic integrity checks must ensure data is not altered without authorization.

6. Medium Sensitivity Data:

    a) Description: Data that poses some risk if compromised, restricted to internal personnel with granted access.

    b) Examples: Internal emails or documents without confidential information, supplier contracts, IT service management or telecommunication information.

    c) Security Measures: Access controls must ensure only authorized internal personnel can access the data. Data must be encrypted during transmission. Regular audits must verify compliance with internal access policies.

7. High Sensitivity Data:

    a) Description: Data with catastrophic impact if compromised, restricted on a need-to-know basis.

b) Examples: User data, financial records (e.g., credit card numbers), PII, medical and biometric data of personnel, employee records, authentication data (e.g., login credentials).

c) Security Measures: Strong access controls, including multi-factor authentication, must be in place. Data must be encrypted both at rest and in transit. Regular security assessments and vulnerability scanning must be conducted. Immediate incident response protocols for data breaches must be established.

8. Data Owners are required to classify data according to Jetzy's classification levels, ensure data is protected according to its classification, review and update data classifications periodically, and grant and review access permissions to ensure only authorized personnel have access.

9. Employees must follow data classification protocols, handle data according to its classification level, report unauthorized access or data breaches immediately to the IT Security department, participate in regular security awareness training sessions, and use appropriate security measures when handling sensitive data.

10. The IT Department must implement and maintain security controls to protect data according to its classification, monitor data access and usage to detect and respond to security incidents, conduct regular audits and security assessments to ensure compliance with data classification policies, and provide support and guidance to data owners and employees on data security best practices.

11. Data classification criteria and processes must be reviewed periodically to ensure effectiveness and alignment with evolving regulatory requirements and business objectives. Reviews must be conducted at least bi-annually, and also as needed.

12. Effective security measures must be in place to ensure that data classified at higher levels is not accessible by those with lower clearance.

13. All classified data must comply with the data protection policies and compliance standards outlined in this document.

10.2 Data Protection

10.3 Credentials

Applications and systems within the organization require authenticated access to various resources. Improper storage of credentials can lead to system compromise. This policy outlines the requirements for securely storing and retrieving

credentials and configurations for all software, hardware, and accounts used within the organization.

1. Credentials and configurations should not be stored in plaintext or using easily reversible encryption within the primary source code or configuration files.
2. Credentials and configurations must be stored in separate files from the application's code or executable body. These files must be protected from being world-readable or writable, reside in distinct directory trees from the executable code (particularly for languages executing from source code), and contain no other code or configurations except the essential functions, routines, or methods for accessing them.
3. Credentials and configuration details must not be accessible via a web server or any public interface, and should not be located in publicly accessible server areas.
4. When credentials or configurations are stored in separate files, they must be accessed immediately before use and cleared from memory promptly after use.
5. Credentials and configurations must be encrypted using algorithms that comply with relevant standards and the encryption requirements specified in this document.
6. Credentials may be stored on secure servers, with a hash or identifier embedded in the application's code.
7. Credentials and configurations can be managed by an authentication or configuration server (e.g., LDAP, Vault) used for secure access management, thus removing the need for direct use in code.
8. Passwords must conform to the organization's password policies outlined in this document.

10.4 Passwords

1. This policy establishes standards for securely managing and protecting all passwords used for any accounts or access on Jetzy systems, networks, applications, platforms, tools, and devices.
2. All personnel, including employees, contractors, vendors, and third-party affiliates with access to Jetzy systems, networks, or non-public information, must adhere to these requirements.

3. Passwords must be at least 18 characters in length, containing at least one lowercase letter, one uppercase letter, and one non-alphabetic symbol.

4. Passwords must not be shared with anyone and are to be treated as sensitive, confidential information.

5. Passwords must not be included in electronic communication, revealed over the phone, or stored in any form other than in authorized password managers. Authorized password managers may be used to securely store and manage all organization-related passwords.

6. Users must employ separate, unique passwords for each work-related account and must not reuse passwords for personal accounts.

7. Multi-factor authentication must be used in conjunction with all these password policies for all work-related and personal accounts.

8. Wherever possible, passwords must be replaced with bio-metric authentication for all work-related and personal accounts.

9. User accounts with system-level privileges must have unique passwords distinct from other accounts held by the user and must employ multi-factor authentication, equivalent to or stronger than 3FA.

10. The "Remember Password" feature must not be enabled on any system, network, application, platform, tool, or device used or developed by the organization.

11. All passwords must be changed at least every 120 days.

12. For password changes or resets, individuals must provide two original proofs of identity as well as credible, verified proof of their authorization for the resource.

13. Default passwords assigned to new personnel or configured systems, networks, devices, tools, and platforms must be generated via GUIDs for each new instance and communicated through secure, encrypted channels.

14. Default passwords must be changed within 24 hours of issuance; failure to do so will result in the account being blocked and deleted.

15. Any suspicion of password compromise must be reported immediately, and relevant passwords changed without delay.

16. Failure to report a compromised password within 24 hours will be considered a policy violation and may have legal consequences.

17. Application developers must ensure that programs support individual user authentication, do not store passwords in clear text and do not transmit passwords over the network in clear text.

18. Regular password audits must be conducted at least every 6 months to test existing systems for vulnerabilities against brute force and other attacks including but not limited to dictionary attacks, rainbow tables etc. Any vulnerabilities found in existing passwords and password policies should be immediately mitigated using appropriate incident response plans, and existing policies revised as needed.

10.5 Encryption

1. All data and information handled by the organization, including but not limited to Personally Identifiable Information (PII), must be encrypted across all assets, functions, and communication channels.

2. Encryption techniques utilized must comply with relevant laws, standards, and organizational policies.

3. Asymmetric encryption methods are preferred over symmetric encryption unless specifically required for certain use cases.

4. Encryption techniques employed must meet or exceed the strength and effectiveness of SHA-256, RSA, AES, ECC, and other specified protocols.

5. The organization must implement and adhere to a Public-Key Infrastructure (PKI), integrating all necessary components into its processes.

6. Encryption of data-at-rest and data-in-transit, including PII, must employ the most advanced and secure techniques available.

7. Both physical and virtual assets must incorporate on-device security encryption measures and utilize cloud encryption methods.

8. All databases, files, disks, and devices containing data-at-rest must be fully secured using techniques such as Full Disk Encryption (FDE) and Transparent Data Encryption (TDE).

9. Internal and external communications related to the organization must utilize End-to-End Encryption (E2EE) to ensure privacy and security.

10. Networks and data-in-transit communications channels must be secured using SSL/TLS, HTTPS, and IPSec protocols to encrypt data packets.

11. Wireless networks within the organization must adhere to WAP3, RSN, CCMP, or stronger wireless security protocols for encrypted communication channels.

12. Remote access to organizational assets and facilities is prohibited unless connections are secured using WAP3, RSN, CCMP, or stronger wireless security protocols.

13. Email and messaging channels utilized by the organization must comply with SMIME, PGP, PEM, or more secure email security protocols.

14. In addition to specified protocols, all networks and communication mediums must comply with relevant laws, standards, and organizational policies.

15. Digital signatures and certificates must be used to encrypt and transmit all confidential or sensitive information, adhering to DSS and other applicable standards.

16. Secure Electronic Transactions (SET) must be employed for all financial web transactions, in alignment with PCI DSS standards and other relevant laws and standards.

17. Third-party encryption tools and software must undergo thorough vulnerability screening before integration into organizational processes.

18. Regular encryption audits must be conducted every six months to identify vulnerabilities, with immediate mitigation of any issues and revision of policies as necessary.

10.6 Application Security

1. The following application security processes apply to all developers and personnel involved in the development, deployment, and maintenance of software applications utilizing the organization's technology stack which includes but is not limited to:

    - Front-end development is carried out using Flutter.
    - Back-end development is performed using Elixir.
    - Version control is managed using Git.
    - Deployment and hosting of applications are on Google Cloud Platform.

2. The organization must conduct regular security training sessions for developers, focusing on secure coding practices relevant to its technology stack, including Flutter for front-end development, Elixir for back-end development, Git for version control, and Google Cloud Platform for cloud deployment.

3. Developers are required to use static application security testing (SAST) tools, compatible with Flutter and Elixir, to scan source code for vulnerabilities and coding errors during the development process.

4. Continuous integration/continuous deployment (CI/CD) pipelines must include automated security checks specific to Flutter and Elixir applications to detect and remediate vulnerabilities before deployment on Google Cloud Platform.

5. The organization must implement dynamic application security testing (DAST) tools capable of assessing Flutter and Elixir applications deployed on Google Cloud Platform by simulating attacks in a production-like environment.

6. Secure coding guidelines and best practices, tailored to Flutter and Elixir development, must be documented and enforced across the organization to ensure consistency and adherence to security standards.

7. Developers must use dependency scanning tools compatible with Flutter and Elixir ecosystems to identify and remediate vulnerabilities in third-party libraries and components.

8. The organization must establish a process for threat modeling, specifically addressing threats relevant to Flutter and Elixir applications deployed on Google Cloud Platform, to prioritize potential security risks.

9. Code review practices must be implemented for Flutter and Elixir codebases to ensure that security vulnerabilities are identified and addressed before code is merged into the main repository on Git.

10. Secure software development frameworks, such as OWASP ASVS and Microsoft SDL, must be adapted and applied to provide guidance and requirements specific to Flutter and Elixir development on Google Cloud Platform.

11. The organization must implement runtime application self-protection (RASP) solutions compatible with Flutter and Elixir to detect and respond to security threats in real-time during application runtime on Google Cloud Platform.

12. Developers must use encryption mechanisms, such as TLS/SSL, compatible with Flutter and Elixir applications, to secure data transmission between client and server components deployed on Google Cloud Platform.

13. Secure authentication mechanisms, such as OAuth, must be implemented for Flutter and Elixir applications deployed on Google Cloud Platform to protect against unauthorized access.

14. The organization must establish incident response plans and procedures tailored to address security incidents specific to Flutter and Elixir applications deployed on Google Cloud Platform.

15. Secure configuration management practices must be followed to ensure that Flutter and Elixir application components deployed on Google Cloud Platform are properly configured and hardened against security threats.

16. Secure coding standards and libraries, specifically designed for Flutter and Elixir development, must be used to prevent common security vulnerabilities, such as SQL injection and cross-site scripting (XSS).

17. The organization must conduct thorough due diligence on vendors and third-party suppliers before engaging in business relationships, assessing their security posture, reputation, and adherence to industry standards.

18. Contractual agreements with vendors and third-party suppliers must include specific security requirements, such as data protection measures, vulnerability management, and incident response protocols.

19. The organization must monitor and evaluate the security practices of vendors and third-party suppliers on an ongoing basis to ensure compliance with contractual agreements and industry regulations.

20. Regular security assessments, including vulnerability scans and penetration tests, must be conducted on third-party software and tools to identify and mitigate potential security risks.

21. The organization must have contingency plans in place to respond to security incidents involving third-party vendors, including communication protocols, incident response procedures, and recovery strategies.

22. Access to sensitive data and systems by third-party vendors must be strictly controlled and monitored, with appropriate access controls, encryption mechanisms, and audit trails implemented.

23. Regular security awareness training must be provided to employees involved in vendor management roles to educate them on the importance of vendor security and best practices for mitigating risks.

24. The organization must maintain an inventory of all third-party vendors and the software tools they provide, along with relevant security documentation, compliance reports, and audit findings.

25. Incident response plans must include procedures for coordinating with third-party vendors during security incidents, including incident notification, information sharing, and collaboration on remediation efforts.

26. Continuous monitoring and auditing of third-party vendors must be performed to detect any changes in their security posture or potential security vulnerabilities that may impact the organization.

27. All software used by the organization, especially security tools and software, must be up-to-date on all Jetzy devices, and forced-update procedures enforced to accomplish this.

28. All software installations requests must be fulfilled using options from the approved list curated by the Information Technology department.

29. If no suitable option aligns with the requester's specific requirements, employees must obtain approval from their manager and submit a written request to the Information Technology department to screen the software.

30. Jetzy employees must refrain from installing any software on Jetzy computing devices within the Jetzy network. Any software installation must be done by the IT personnel and must be recorded.

10.7 Web Application Security

1. All web applications must undergo security assessments to identify potential vulnerabilities and mitigate risks before production deployment.

2. Security assessments are required for new or major application releases, third-party or acquired applications, point releases, and patch releases, adhering to the specified assessment levels.

3. Annual security reviews must be conducted for all web applications to evaluate potential risks in functionality and architecture.

4. Emergency releases may bypass security assessments temporarily, but the assumed risk must be documented, and the application assessed promptly. Approval for emergency releases must be granted by the Chief Information Officer or an authorized delegate.

5. Discovered security issues must be mitigated based on risk levels defined by the OWASP Risk Rating Methodology. High-risk issues must be addressed immediately or mitigated before deployment. Medium-risk issues must be scheduled for remediation, and low-risk issues must be reviewed and scheduled accordingly.

6. The Information Security (InfoSec) team is required to perform all web application security assessments using approved tools and methodologies. Assessment levels include:

a) Full Assessment: Comprehensive testing for all known web application vulnerabilities using both automated and manual tools, in accordance with the OWASP Testing Guide. Manual penetration testing will validate discovered vulnerabilities.

b) Quick Assessment: Automated scans for at least the OWASP Top Ten web application security risks.

c) Targeted Assessment: Verification of vulnerability remediation changes or new application functionality.

7. All findings from web application security assessments are confidential and must be distributed on a need-to-know basis. External distribution of findings requires approval from the Chief Information Officer.

8. Relationships within multi-tiered applications identified during the scoping phase must be included in the assessment unless explicitly excluded and documented.

9. The InfoSec team is required to verify compliance with this policy through various methods, including business tool reports, audits, and feedback. Exceptions to the policy must be pre-approved by the InfoSec team.

10. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment. Non-compliant applications may be taken offline until a formal assessment is conducted.

11. Web application assessments are integral to the change control process, and all application releases must comply with this policy.

12. The following standards and methodologies must be referenced: OWASP Top Ten Project, OWASP Testing Guide, and OWASP Risk Rating Methodology.

10.8 Security Continuous Monitoring

1. All information systems must generate and store logs for critical activities, including user logins, data access, system modifications, and security incidents.

2. Logs must be securely stored in a centralized logging system to prevent tampering and ensure data integrity.

3. Access to logging systems must be restricted to authorized personnel, with strict access controls and regular access reviews.

4. Logs must be retained for a period defined by organizational policies and relevant legal or regulatory requirements.

5. Logging systems must capture sufficient detail to enable effective monitoring, incident response, and forensic analysis.
6. Logs must include sufficient audit information to address the following:
    a) What activity was performed.
    b) Who or what performed the activity, and where or on what system the activity was performed (subject).
    c) What the activity was performed on (object).
    d) When the activity was performed.
    e) What tools were used for the activity.
    f) The status (such as success vs. failure), outcome, or result of the activity.
7. Logs shall be created for the following activities:
    a) Creating, reading, updating, or deleting confidential information, including passwords.
    b) Creating, updating, or deleting non-confidential information.
    c) Initiating or accepting network connections.
    d) User authentication and authorization, including user login and logout.
    e) Granting, modifying, or revoking access rights.
    f) System, network, or service configuration changes, including software updates.
    g) Application process startup, shutdown, restart, or abnormal termination.
    h) Detection of suspicious or malicious activity by security systems (e.g., IDS/IPS, antivirus).
8. All logs must include the following elements:
    a) Type of action (e.g., authorize, create, read, update, delete, network connection).
    b) Subsystem performing the action (e.g., process name, transaction identifier).
    c) Identifiers for the subject (e.g., user name, computer name, IP address, MAC address).
    d) Identifiers for the object (e.g., file names, database records, IP address).
    e) Before and after values when updating data, if feasible.

f) Date and time of the action, including relevant time-zone information.

g) Whether the action was allowed or denied by access-control mechanisms, including reasons for denial.

9. Logs must be formatted and stored to ensure integrity and support enterprise-level analysis and reporting, using mechanisms such as:

a) Microsoft Windows Event Logs collected by a centralized system.

b) Logs sent via syslog protocols to a centralized system.

c) Logs stored in an ANSI-SQL database that generates compliant audit logs.

d) Other open logging mechanisms supporting the above requirements.

10. Systems must monitor and analyze logs in real-time for signs of suspicious activity, anomalies, or potential security breaches.

11. Regular audits of logging systems must be conducted to ensure compliance with logging standards and identify gaps or weaknesses.

12. Logs related to security incidents must have additional security measures to prevent unauthorized access and ensure their integrity.

13. Automated alerting mechanisms must notify relevant personnel of critical security events or anomalies detected in logs.

14. Log data must be encrypted during transmission and storage to ensure confidentiality and integrity.

15. Backup and recovery processes must be in place to ensure log data can be restored in the event of data loss or system failure.

16. Employees responsible for managing and analyzing logs must receive appropriate training to understand the importance of logging and how to effectively use logging tools.

17. The organization must establish a policy for regular review and deletion of logs no longer required, in compliance with retention policies and legal requirements.

11 Operational Security

11.1 Access Controls

1. The organization must establish and document cybersecurity roles and responsibilities for all workforce members and third-party stakeholders, including suppliers, customers, and partners.
2. Identities and credentials for authorized devices, users, and processes must be meticulously issued, managed, verified, revoked, and audited.
3. Access permissions and authorizations must be meticulously managed, ensuring strict adherence to the principles of least privilege and separation of duties.
4. Session management procedures must be implemented across organizational systems to regulate and monitor active sessions effectively.
5. The organization is required to adopt and enforce the Authentication Tokens Standard to ensure secure authentication processes.

11.2 Incident Response Planning

1. A dedicated incident response team must be formed to develop and implement comprehensive incident response plans.
2. The organization must assess its assets and resources to compile a thorough list of potential violations, incidents, and attacks.
3. Third-party services should be engaged to assist in testing the effectiveness of current systems in safeguarding against incidents and recovering from disasters.
4. Incidents must be classified based on their impact, likelihood, and effect on organizational resources and functions.
5. Intrusion detection and prevention systems, as well as recovery methods, must be identified and implemented for each incident.
6. Protocols, procedures, and reporting tools must be established for reporting, preventing, identifying, containing, rectifying, and recovering from incidents.
7. Regular testing and monitoring of security measures must be conducted to ensure effectiveness against evolving threats.

11.3 Risk Management

1. Based on data classification, the organization must develop tailored security measures for data storage, transmission, and use, including encryption techniques, authentication methods, and access controls.
2. Role-based or attribute-based access controls must be established for personnel, specifying security requirements, session limits, authorized equipment/resources, authentication requirements, and access failure allowances.
3. The organization should identify and provide necessary security certifications and training for personnel.
4. Thorough pentesting and risk assessments must be conducted to identify vulnerabilities in the organization's security infrastructure.
5. The organization must research and adopt appropriate security software, hardware, and techniques to address identified security needs.
6. Network diagrams must be revised to incorporate best practices such as network segmentation and internet security protocols.
7. Physical security measures should be revised and enhanced as needed, utilizing appropriate equipment and tools.
8. Redundancy and fail-over systems must be implemented based on organizational use cases and requirements.
9. A comprehensive security plan with budget, timelines, and deliverables must be proposed and implemented based on research, findings, and security requirements.

11.4 Supply Chain Risk Management

1. Suppliers and third-party partners of information systems, components, and services must be identified, prioritized, and assessed using a cyber supply chain risk assessment process.
2. Routine assessments of suppliers and third-party partners must be conducted using audits, test results, or other evaluations to confirm compliance with contractual obligations.
3. Response and recovery planning and testing must be conducted collaboratively with suppliers and third-party providers.

11.5 Disaster Recovery & Business Continuity

1. Management is required to provide financial support and actively engage in disaster recovery planning efforts to establish a robust contingency plan for Jetzy.
2. A comprehensive Disaster Recovery Plan (DRP) must be formulated, executed, and regularly updated to enable the restoration of IT systems, applications, and data in the event of a major outage.
3. IT Management Staff are responsible for developing, testing, and maintaining the Disaster Recovery Plan.
4. The Disaster Recovery Plan must encompass the following contingency plans:
    a) **Computer Emergency Response Plan:** Specify contact details, timing for communication, and immediate response actions for specific events.
    b) **Succession Plan:** Outline the flow of responsibility in the absence of regular staff members.
    c) **Data Study:** Provide detailed information on stored data, including criticality and confidentiality.
    d) **Criticality of Service List:** Prioritize all provided services and outline the recovery order for short-term and long-term scenarios.
    e) **Data Backup and Restoration Plan:** Specify data backup details such as content, media, storage location, backup frequency, and recovery procedures.
    f) **Equipment Replacement Plan:** Describe the necessary equipment for service resumption, prioritize the order of procurement, and identify procurement sources.
    g) **Mass Media Management:** Designate a responsible individual for media communication and provide guidelines on appropriate information release.
    h) **Business Continuity Strategies:** Develop strategies to sustain business operations during disruptions.
    i) **Public Relations Management:** Assign responsibility for managing public relations during and after incidents.
    j) **Reputation Repair:** Develop plans to restore the organization's reputation post-incident.
    k) **Stakeholder Communication:** Communicate recovery activities to internal and external stakeholders, executive, and management teams.

5. Management must allocate time for annual table-top exercises to assess the effectiveness of the disaster recovery plan implementation.

6. The Disaster Recovery Plan must undergo annual review and updates to ensure continued effectiveness and relevance.

12 Personnel Security

12.1 Acceptable Use

1. All personnel with access to Jetzy's network are required to strictly adhere to the acceptable use policy. They must utilize organizational resources responsibly and exclusively for legitimate business purposes.

2. Unauthorized activities such as downloading pirated software, accessing unauthorized websites, or utilizing organizational resources for personal gain are strictly prohibited. Personnel must refrain from engaging in such activities.

3. Personnel must ensure the security and integrity of all physical devices and systems provided by the organization, including computers, mobile devices, and network infrastructure. They are required to follow organizational guidelines for proper use and maintenance.

4. Unauthorized access, modification, or destruction of any physical device or system within the organization is strictly prohibited. Personnel must immediately report any suspicious activity or security incidents involving organizational devices to the IT Security department.

5. All software platforms and applications used within the organization must be authorized and properly licensed. Personnel are required to use only approved software provided by the organization.

6. The installation or use of unlicensed or unauthorized software on organizational devices is prohibited. Personnel must adhere to software usage policies and comply with licensing agreements.

7. Before using external information systems such as cloud services and third-party applications, personnel must catalog and obtain approval from the organization. They are required to ensure compliance with the organization's security standards and data protection policies for these systems.

8. Personnel must control and monitor access to external information systems to prevent unauthorized access and data breaches. Strong authentication methods must be used, and access control policies must be followed.

9. The use of removable media must be restricted according to organizational policy. Personnel are required to use encrypted removable media when transferring sensitive data.

10. Unauthorized use of removable media is prohibited. Personnel must follow procedures for the secure disposal of removable media to prevent data leakage.

11. Personnel must comply with all laws and regulations regarding copyrighted, licensed, and other intellectual property. The use of such materials must adhere to licensing agreements and organizational policies.

12. Unauthorized copying, distribution, or use of copyrighted or licensed materials is strictly prohibited. Proper authorization must be obtained before using any intellectual property belonging to the organization or third parties.

12.2 Vendor and Third-Party Security

1. Personnel responsible for vendor and third-party management must ensure that all vendors and third-party partners undergo a security assessment before being granted access to Jetzy's network or data.

2. Regular audits and evaluations of vendors and third-party partners must be conducted by personnel to verify ongoing compliance with security requirements.

12.3 Monitoring

1. The Information Technology Department must monitor Internet use from all computers and devices connected to Jetzy's corporate network. The monitoring system must record source IP addresses, dates, times, protocols, and destination sites or servers. User IDs of the person initiating the traffic, where possible, must also be recorded. Internet use records must be preserved for 180 days.

2. General trending and activity reports must be available to any employee upon request to the Information Technology Department. The Computer Security Incident Response Team (CSIRT) may access all reports and data as necessary to respond to security incidents. Reports identifying specific users, sites, teams, or devices will only be provided to associates outside the CSIRT upon written or email request from a Human Resources representative to Information Systems.

3. The Information Technology Department must block access to Internet websites and protocols deemed inappropriate for Jetzy's corporate environment. Specific categories of websites and protocols must be blocked, including but not limited to adult content, advertisements, gambling, and hacking-related sites.

4. The Information Technology Department must periodically review and recommend changes to web and protocol filtering rules. Human Resources must review these recommendations and decide on any changes. Changes must be recorded in the Internet Use Monitoring and Filtering Policy.

5. Employees may request the unblocking of mis-categorized sites by submitting a ticket to the Information Technology help desk. IT personnel must review and unblock mis-categorized sites upon verification.

6. Employees needing access to blocked sites for business purposes must request approval from their Human Resources representative. Approved requests will be forwarded to Information Technology for unblocking, with exceptions tracked and reported upon request.

7. Personnel must be aware that event data are collected and correlated from multiple sources and sensors to detect potential cybersecurity events.

8. Personnel must cooperate with measures to detect unauthorized connections, devices, and software.

9. Personnel must cooperate with vulnerability scanning, auditing, and security logging standards.

10. Personnel must cooperate with measures taken to detect and mitigate malicious code.

12.4 Incident Response

1. Personnel must report incidents promptly in accordance with established criteria and respond using predefined protocols.

2. Personnel must regularly conduct, maintain, and test backup procedures to ensure data integrity and availability.

3. Patch management and response strategies must incorporate lessons learned from previous incidents and be updated accordingly by responsible personnel.

12.5 Employee Awareness

1. All personnel must receive training on their roles and responsibilities in maintaining information security within the organization.

2. Personnel must attend regular security awareness training sessions to stay informed about the latest security threats and best practices.

3. Employees must immediately report any security incidents or suspicious activities to their supervisor or the IT Security department.

12.6 Limitations of Liability

1. Personnel must acknowledge that Jetzy will not be held liable for any loss or damage resulting from unauthorized or improper use of organizational resources.

13 Implementation Plan

13.1 Planning

1. Create a dedicated security planning task force in the Information Security department also comprising representatives from IT, security, legal, and relevant business units.
2. Set a timeline for developing a comprehensive information security implementation plan.
3. Inventory all organizational resources, assets, networks, software, hardware, devices, types, locations etc used for all organizational processes and create a comprehensive data and assets registery.
4. Classify all types of data and asssets in the register based on their confidentiality, integrity, availability and business importance to the organization.
5. Develop a comprehensive list of all current on-premise and remote organizational personnel, staff, employees, departments, third-party contractors, vendors, and all associated individuals and sectors of the organization in a personnel registery.
6. Classify all personnel registry into groups based on their roles, functions, jobs, tasks, authorizations, access etc.
7. Assess the current security awareness and training level of different groups of organization personnel through feedback and assessments, or other appropriate methods.
8. Devise a detailed semantics and networks diagram for the entire organization, as well as a detailed blueprint diagram of its physical facilities.
9. Collect all information related to current physical, network, INFOSEC, COMSEC, OPSEC and personnel security measures, tools, techniques and policies already enforced on the organization as well as their level of compliance.
10. Create a detailed list of global and local compliance standards, laws, protocols, best practices etc that the organization must adhere to.
11. Present your findings at the end of the researching phase to now develop a comprehensive implementation plan.

13.2 Risk Assessment

1. Based on the data classification, develop the most appropriate data storage, data transmission, and data use security measures for each type of data, including but not limited to appropriate encryption techniques, data authentication methods, transmission protocols and channels, requirements for authorizing access to these data, logging and monitoring frequency and details, back-up and redundancy requirements of this data, session limits of accessing this data, and any physical security requirements that may be needed for it.

2. Based on the personnel registry, develop a detailed role-based or attribute-based access controls list along with security requirements, session limits, authorized equipment/areas/resources, requirements for authentication, minimum number of access failure allowance, and any special authorizations for each access control. Implement separation of duties and least privileges to maintain security.

3. Also determine which security certifications and training is needed by organization personnel.

4. Hire and conduct a thorough pentesting and risk assessment of the entire organization to identify vulnerabilities in the organization's current security.

5. Research and determine the best security software, hardware, techniques, methods, tools, devices and equipment needed for each identified area of security.

6. Revise the network diagram of the organization to determine incorporation of best network security practices including but not limited network segmentation, internet security protocols, packet analysis and scanning tools etc.

7. Determine appropriate revisions to the physical security of the organization and determine the best equipment, tools and measures for accomplishing that.

8. Determine the appropriate amount and nature of redundancy and failover systems that your organization needs for each individual organization use case.

9. Based on all research, findings and security requirements, propose a budget and comprehensive security plan with timelines and deliverables for implementing information security in your organization.

13.3 Implementation

1. Once the budget for security measures implementation is approved, enforce your plan in phased deployments.
2. Install new equipment, systems, resources, hardware, software, tools, devices, platforms, scanning and monitoring equipment in appropriate timelines.
3. Migrate from old to new systems based on strategically decided downtime for departments/function/teams within the organization to not affect business operations.
4. Educate personnel on using new systems, specifically on their security features.
5. Update and modify the implementation plan based on emerging circumstances to best enhance security during the implementation phase.

13.4 Incident Response & Disaster Recovery

1. Create a dedicated team to develop incident response plan and implement disaster recovery measures.
2. Assess the organization's assets and resources to develop an extensive list of violations, incidents, attacks that can occur.
3. Involve third-party services to assist in testing current systems for effectiveness in safeguarding incidents and recovering from disasters.
4. Classify this list of incidents based on their impact and likelihood, as well as their affect on the organization resources and functions, and causes.
5. Devise a list of appropriate intrusion detection prevention systems and recovery methods for each incident.
6. Develop a list of protocols and procedures and reporting tools to be followed by all involved individuals to report, prevent, identify, contain, rectify and recover from any damage to data or assets caused by these incidents.
7. Conduct thorough testing to test the new proposed and implemented features that are meant to safeguard against these incidents and disasters.
8. Continuously revise and monitor systems for new evolving threats and test the effectiveness of security measures against them.

13.5 Reviewal, Updates & Modifications

1. Implement continuous monitoring and logging of all organization systems, networks, assets, resources etc.
2. Regularly review organizational logs for anomalies and incidents and revise and modify security measures based on effectiveness against safeguarding against those on a timely basis.
3. Scan and implement patch management on all software used in the organization on an immediate basis.
4. Test organization security systems and conduct risk assessments, pentests, personnel security training and awareness sessions and assessments at least bi-annually, and also as needed.
5. Review and modify the security policy at least bi-annually or as needed to ensure compliant and effective organization-wide security of information, data and assets.

14 Compliance

The organization must comply with all information security laws, standards, protocols and regulations it is subjected to in the United States of America, Pakistan, Canada as well as any other areas of its operation.

14.1 Industry Standards

1. ISO 27001 and ISO 9001 Compliance: All departments must adhere to ISO 27001 standards for information security management and ISO 9001 standards for quality management. The IT department is responsible for ensuring that all information security measures comply with ISO 27001, while the Quality Assurance team must ensure compliance with ISO 9001.

2. NIST Cybersecurity Framework: The IT Security team must implement and maintain practices outlined in the NIST Cybersecurity Framework to manage and reduce cybersecurity risk across all organizational processes.

3. GIAC Certification: IT and security personnel must attain and maintain GIAC certifications to validate their expertise in IT security and ensure they are equipped with up-to-date knowledge and skills.

4. IEEE 802.11 Compliance: The Network Operations team must ensure all wireless networking equipment and protocols comply with IEEE 802.11 standards to maintain secure and reliable wireless communications.

5. SOC 2 and SOC 3 Compliance: The IT and Compliance departments must ensure that all systems handling customer data comply with SOC 2 and SOC 3 standards to maintain data integrity, confidentiality, and privacy. Service level agreements must reflect these compliance requirements.

6. CompTIA Social Media Security: Marketing and Social Media teams must follow CompTIA Social Media Security guidelines to secure social media accounts and protect against related threats.

7. NIST Special Publication 800-53: The IT department must implement security and privacy controls as defined in NIST SP 800-53 to protect organizational information systems and data.

8. PCI-DSS Compliance: The Finance and IT departments must ensure that all processes involving payment card information comply with PCI-DSS standards to secure the handling of payment card data.

9. OWASP Best Practices: The Web Development and IT Security teams must follow OWASP best practices for web application security to protect against vulnerabilities and threats in web applications.

10. NIST FIPS 140-2 Standards: The IT Security team must use encryption methods that comply with NIST FIPS 140-2 standards to ensure the secure transmission and storage of sensitive data.

11. Digital Signature Standard (DSS): The Legal and IT departments must implement digital signatures in accordance with the DSS to ensure the authenticity and integrity of digital documents.

12. National Cyber Security Policy of Pakistan:All operations in Pakistan must comply with the National Cyber Security Policy 2021 to enhance cybersecurity measures and protect against cyber threats.

13. All departments must ensure compliance with relevant industry standards specific to the regions in which they operate, beyond the USA, Canada, and Pakistan. This includes adhering to local cybersecurity and information management standards to ensure comprehensive protection and operational efficiency.

14.2 Data Protection Laws

1. GDPR Compliance: The Data Protection Officer (DPO) must ensure that all data processing activities involving EU citizens' data comply with the GDPR to protect data privacy and rights. Note that although Europe is not one of Jetzy's main locations of operations, its laws are a global standard that the organization must adhere to in light of future goals of expansion.

2. CCPA Compliance: The Privacy Officer must ensure that all data collection and processing activities comply with the CCPA to protect the privacy rights of California residents.

3. PIPEDA Compliance: The Privacy Officer must ensure compliance with PIPEDA for all personal data handling activities involving Canadian citizens to protect their data privacy rights.

4. COPRA Compliance: The Privacy Officer must prepare for and ensure compliance with the COPRA for future federal data privacy regulations in the United States.

5. The Data Protection Officer (DPO) and Privacy Officer must ensure compliance with data protection laws specific to the regions where the organization operates, beyond the USA, Canada, and Pakistan. This

includes adhering to local regulations to safeguard personal data and privacy.

14.3 Service Level Agreement

1. SOC 2 and SOC 3 Service Level Agreements: The Compliance and IT departments must ensure that all service level agreements (SLAs) include requirements for SOC 2 and SOC 3 compliance to guarantee that customer data is managed with appropriate security controls and privacy measures.

2. The Compliance and IT departments must ensure that SLAs comply with local regulations and standards specific to the regions in which the organization operates, beyond the USA, Canada, and Pakistan. This includes aligning SLAs with local requirements to ensure service quality and regulatory compliance.

14.4 Conclusion

In conclusion, this information security policy serves as a comprehensive framework for safeguarding Jetzy's assets, data, and operations against cyber threats and risks. By implementing the outlined strategies and procedures, Jetzy aims to enhance its security posture, protect user privacy, ensure regulatory compliance, and mitigate the impact of incidents and disasters.

With a dedicated focus on planning, risk assessment, implementation, incident response, and compliance, Jetzy is committed to fostering a secure and resilient organizational environment. By continuously reviewing, updating, and adapting security measures, Jetzy will stay proactive in addressing emerging threats and evolving regulatory requirements.

Through collaboration across departments and adherence to industry standards, Jetzy will strive to maintain the highest standards of information security and data protection. By instilling a culture of security awareness and accountability among employees, Jetzy will reinforce the importance of information security as a core business priority.

Ultimately, this policy reflects Jetzy's unwavering commitment to protecting its assets, data, and reputation in an increasingly complex and interconnected digital landscape. By embracing a proactive and holistic approach to information security, Jetzy will continue to earn the trust and confidence of its customers, partners, and stakeholders.

15 References

The following references were used in the development of this Information Security Policy:

- SANS Institute for Cybersecurity Training. (n.d.). Information Security Policy Templates. Retrieved from https://www.sans.org/information-security-policy/
- Ministry of Information Technology & Telecommunication, Government of Pakistan. (2021). National Cyber Security Policy. Retrieved from https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf
- Pakistan Computer Emergency Response Team (PKCERT). (n.d.). Retrieved from https://pkcert.org/
- Jetzy. (n.d.). Privacy Policy. Retrieved from https://jetzyapp.com/privacy.html
- National Institute of Standards and Technology (NIST). (2021). NIST Cybersecurity Framework Policy Template Guide. Retrieved from https://www.nist.gov/cyberframework
- Habib Bank AG Zurich. (n.d.). Information Security Policy. Retrieved from internal documents.