UBONA CORPORTATE SECURITY WHITE PAPER

Standard and Practices

Contents

Introduction 3
Security at Ubona 3
People Security 3
- Security Training 4
- Background Checks 4
- Continuous Education 4

Network, Application and Infrastructure Security 5
- Security of the Data 5
- Access Control 5
- Endpoint Security Protection 5
- Monitoring 6
- Password Policy 6
- Securing Privileged Access 6
- Vulnerability Management 7
- Penetration Testing 7
- Security By Design 7

Physical Security 8
- Office Security 8
- Data Center Security 8

Risk Management 8
Business Continuity Plan & Disaster Recovery 8
- Business Continuity 8
- Disaster Recovery 9
- Incident Response Plan 9
- Vendor Management 9

About Ubona 10

Introduction

In the era of digital transformation, customer engagement stands at the forefront of business success. As companies strive to meet the evolving needs and expectations of their clientele, innovative solutions emerge to streamline communication channels and enhance the overall customer experience. Ubona, a pioneer in cloud-based contact center solutions, has been at the forefront of this revolution, empowering leading Indian companies to redefine customer engagement through its cutting-edge Visual IVR BOT and Cloud Telephony service.

Security at Ubona

As a software developer and technology provider, Ubona Technologies places a strong emphasis on security. Our security strategy is carefully crafted and implemented across the entire organization. We have dedicated teams and an Information Security committee overseeing our security standards and controls, ensuring that our critical company data and assets are protected at a high level.

Ubona Technologies holds ISO/IEC 27001:2022 certification for our Information Security Management System (ISMS), demonstrating our commitment to international best practices in information security. Additionally, our Software as a Service offerings have achieved SOC 2 Type 2 compliance and RBI SAR/DL compliance, providing assurance to our clients regarding the security, availability, and processing integrity of our systems.

We regularly review and audit our internal systems storing customer data to ensure compliance with security policies and guidelines. Our comprehensive information security framework covers various aspects including asset management, access control, physical security, network security, and incident response. These policies and standards are approved by management and accessible to all Ubona Technologies employees, underscoring our dedication to maintaining a secure environment for our customers and their data.

People Security

At Ubona, our employees play a crucial role in maintaining our commitment to security. We take several measures to ensure the integrity of our team, including

conducting pre-employment background checks in accordance with local laws. Additionally, we have robust onboarding processes for new employees and ongoing training programs to keep our team updated on the latest security protocols and best practices. These training sessions may cover topics such as:

Security Training

At Ubona Technologies, we prioritize the ongoing training and awareness of our employees regarding company policies and security practices. This includes annual security training sessions and regular updates on security awareness activities.

As part of our comprehensive onboarding process, all new employees at Ubona Technologies undergo training and certify their agreement to comply with our information security policies. This ensures that every member of our team understands their role in upholding our security standards from day one.

Moreover, we require all Ubona Technologies employees to successfully complete annual privacy training. This training covers essential topics such as privacy best practices and compliance requirements under relevant privacy laws, including the Digital Personal Data Protection Act (DPDPA) and General Data Protection Regulation (GDPR).

For further details about our privacy practices, we invite you to visit our Privacy Center at www.ubona.com/privacy-center. There, you can find comprehensive information regarding how we handle and protect personal data, demonstrating our commitment to transparency and compliance with privacy regulations.

Background Checks

The hiring process for candidates at Ubona Technologies includes external reference checks. These checks may also include verification of education and previous employment history.

Where local labor law or statutory regulations permit, Ubona Technologies may also conduct criminal, credit, and Address checks, depending upon the specific jurisdiction and position.

Continuous Education

At Ubona Technologies, our security team keeps employees informed about emerging threats and advises on phishing campaigns. Employees are urged to promptly report any security incidents to the Information Security or Information Technology departments. Additionally, we maintain a clear Acceptable Use Policy for all employees and contractors, outlining the proper use of our IT assets.

Network, Application and Infrastructure Security

At Ubona, we take every precaution to safeguard customer information in all its forms. We implement a variety of security measures, including administrative, physical, technical, and organizational controls. These measures are carefully designed to prevent unauthorized access, modification, disclosure, or deletion of customer data, ensuring compliance with all relevant laws and regulations. Our commitment to protecting customer information is unwavering, reflecting our dedication to maintaining trust and confidentiality in every aspect of our operations.

Security of the Data

At Ubona Technologies, we prioritize the security of your data at every step. We employ robust encryption protocols such as TLS and AES 256 to protect data both in transit and at rest, ensuring it remains confidential and secure. Access to sensitive information is strictly controlled through comprehensive access control mechanisms, allowing only authorized personnel to access data. Additionally, we regularly purge unnecessary data to minimize the risk of unauthorized access and maintain data integrity. Your trust and the security of your data are paramount to us, and we continuously strive to uphold the highest standards of data protection.

Access Control

At Ubona Technologies, we prioritize strict access control measures to safeguard sensitive information. Our approach is based on the principle of "need to know" and "least privilege," meaning employees are granted access only to the data and systems necessary for their specific roles. Additionally, we enhance security through Multi-Factor Authentication (MFA), adding an extra layer of protection against unauthorized access.

Endpoint Security Protection

At Ubona Technologies, we prioritize endpoint security to safeguard against potential threats. Our approach includes utilizing BitLocker encryption to protect data stored on devices, ensuring confidentiality even if the device is lost or stolen. We also employ robust antivirus software to detect and mitigate malware and other malicious software. Additionally, we utilize Extended Detection and Response (XDR) solutions to provide comprehensive threat detection and response capabilities across our network, endpoints, and cloud environments. With these layers of protection in place, we maintain a secure computing environment, safeguarding both company and client data from potential security risks.

MONITORING

At Ubona Technologies, we employ a Security Information and Event Management (SIEM) system to monitor our network and systems effectively. SIEM allows us to collect, analyze, and correlate security events in real-time, enabling us to detect and respond to potential threats promptly. By continuously monitoring our IT infrastructure, applications, and user activity, we can identify suspicious behavior, security incidents, and policy violations, ensuring the integrity and security of our systems and data. SIEM plays a crucial role in our proactive approach to cybersecurity, allowing us to stay one step ahead of potential threats and protect our organization from harm.

PASSWORD POLICY

At Ubona Technologies, we enforce a stringent password policy to enhance security across our systems. Our policy includes requirements for password complexity, ensuring that passwords are sufficiently strong to resist unauthorized access. Additionally, passwords expire periodically, prompting users to regularly update them and further bolster security. To mitigate the risk of unauthorized access, we implement measures to block multiple wrong attempts, preventing brute force attacks and unauthorized entry into our systems. By adhering to these practices, we maintain a robust defense against potential security threats and safeguard our organization's sensitive information.

SECURING PRIVILEGED ACCESS

At Ubona Technologies, securing privileged access is paramount. We employ stringent controls, such as Multi-Factor Authentication (MFA) and Privileged Access Management (PAM), to limit access to critical systems and data. We are enforcing strict authentication and authorization measures, we ensure that only authorized individuals can access privileged accounts, reducing the risk of unauthorized activity and potential security breaches.

Vulnerability Management

At Ubona Technologies, we prioritize vulnerability management to proactively identify and mitigate potential security risks. To achieve this, we collaborate with CERT-IN empaneled vendors, leveraging their expertise and resources to conduct comprehensive vulnerability assessments and penetration testing. By partnering with certified vendors, we ensure thorough and effective vulnerability management practices, strengthening our defenses against cyber threats and enhancing the overall security posture of our organization.

Penetration Testing

At Ubona Technologies, we prioritize the security of our systems through regular penetration testing conducted by CERT-IN empaneled vendors. This rigorous testing helps identify potential vulnerabilities and weaknesses in our infrastructure, applications, and networks. By partnering with certified vendors, we ensure thorough assessments and actionable insights to strengthen our defenses against cyber threats. Through penetration testing, we continuously enhance our security measures, ensuring the resilience and integrity of our systems against evolving threats.

Security By Design

At Ubona we ensure that the code is free from common vulnerabilities. We Follow secure coding guidelines such as those provided by OWASP (Open Web Application Security Project). Regularly train developers on secure coding practices and conduct code reviews to identify and fix security issues. Ubona Incorporate static and dynamic code analysis tools to detect vulnerabilities in the code. Conduct regular security testing, including penetration testing and vulnerability assessments, to identify and address security flaws.

Physical Security

Office Security

At Ubona Technologies, we prioritize office security to ensure the safety of our employees and assets. Our comprehensive security measures include biometric access control systems, such as fingerprint or facial recognition, to restrict entry to authorized personnel only. Additionally, CCTV surveillance cameras are strategically placed throughout our premises to monitor and record activity, enhancing overall security and providing a deterrent against unauthorized access or incidents. Furthermore, we maintain a visitor register and issue visitor ID cards to track and authenticate external visitors, allowing us to maintain a secure environment while facilitating guest access when necessary. These measures collectively contribute to a safe and secure office environment, fostering peace of mind for everyone within our facilities.

Data Center Security

At Ubona Technologies, our data center security is robust. We leverage AWS, Azure, and co-location data centers, all following industry-standard security practices. This includes strict access controls, encryption, and continuous monitoring, ensuring the utmost protection for our infrastructure and customer data.

Risk Management

Ubona conducts information security risk assessments on an annual basis, with the results being included in the annual mitigation plan, which is presented to and monitored by Ubona's Audit Committee.

Business Continuity Plan & Disaster Recovery

Business Continuity

At Ubona Technologies, we prioritize business continuity to ensure seamless operations, even in the face of unforeseen challenges or disruptions. Our comprehensive strategy encompasses proactive planning, redundancy measures, and contingency protocols to minimize downtime and maintain essential services. By regularly assessing risks, implementing resilient infrastructure, and conducting drills

and simulations, we remain prepared to swiftly respond to any adverse events and uphold our commitment to delivering uninterrupted services to our customers.

Disaster Recovery

At Ubona Technologies, we prioritize disaster recovery by implementing a robust strategy that involves replicating data across different geographic zones. This approach ensures redundancy and resilience, minimizing the risk of data loss or service interruption in the event of a disaster affecting a specific zone. By maintaining master and replica data in different zones, we enhance our ability to recover quickly and continue providing uninterrupted services to our customers, even in the face of unforeseen events or disruptions.

Incident Response Plan

At Ubona Technologies, we prioritize a proactive approach to incident response, guided by a comprehensive incident response plan (IRP) overseen by our Incident Response Team (IRT). This policy outlines the procedures for identifying, classifying, reporting, remediating, and mitigating security incidents across all stages of the incident response lifecycle, including post-incident assessments. By adhering to this plan, we ensure swift and effective responses to security incidents, minimizing their impact and preventing future occurrences, thereby safeguarding our systems, data, and stakeholders.

Vendor Management

Vendor management is a critical aspect of operations at Ubona Technologies. We carefully select and oversee our vendors to ensure they meet our standards for quality, security, and compliance. Our approach involves thorough vetting, contract negotiation, performance monitoring, and relationship management to maximize value and mitigate risks associated with third-party partnerships. By maintaining proactive and transparent communication with our vendors, we foster mutually beneficial collaborations that contribute to the success and resilience of our organization.

About Ubona

Ubona is a leading technology company specializing in customer engagement and business optimization solutions. With a focus on innovation and customer-centricity, we offer a comprehensive suite of products and services, including cloud-based contact center solutions, AI-driven chatbots, and visual IVR systems. Our team of experts is dedicated to delivering seamless and personalized experiences across multiple communication channels. At Ubona, we are committed to excellence, reliability, and customer satisfaction, helping businesses thrive in the digital age through optimized customer interactions, improved operational efficiency, and revenue growth. To learn more, visit us at www.ubona.com.