Dstny Security White Paper

Exported on 27 June, 2023

dstny

Table of Contents

1 Executive Summary

Dstny is committed to maintaining the highest standards of security to protect our systems, customer data, and sensitive information. This executive summary provides an overview of our comprehensive security practices, outlining the key measures and protocols we have implemented to ensure the confidentiality, integrity, and availability of our services.

Our security framework encompasses a multi-layered approach that addresses various aspects of security, including network security, data encryption, access controls, incident response, and compliance with industry standards and regulations. By implementing these measures, we strive to create a secure environment for our customers and maintain their trust in our services.

Highlights of our security practices include:

1. **Network Security**: We employ robust network security measures, such as firewalls, fraud detection systems, and regular vulnerability assessments, to safeguard our infrastructure and communication channels.
2. **Data Encryption**: All sensitive data transmitted between our services and our customers' systems is encrypted using industry-standard protocols, ensuring the confidentiality and integrity of the data in transit.
3. **Access Controls**: We enforce strict access controls, including strong authentication mechanisms and role-based access controls, to prevent unauthorized access to our systems. Regular access reviews are conducted to maintain the security of our infrastructure.
4. **Incident Response**: Our operational organization promptly responds to security incidents, following established processes for reporting, investigation, and containment. This ensures the quick resolution of incidents and minimizes their impact on our systems and customer data.
5. **Compliance**: We adhere to industry best practices and comply with relevant regulations and standards to ensure the highest level of security. Regular audits and assessments are conducted to verify the effectiveness of our security measures.

At Dstny, we consider security a top priority and continuously monitor and improve our security practices to stay ahead of emerging threats. By prioritizing the confidentiality, integrity, and availability of our services, we aim to provide our customers with a secure and reliable platform for their business needs.

Please note that this executive summary provides a high-level overview of our security practices. For detailed information, please continue reading the full white paper below.

2 Content

2.1 Context

For the purpose of this document, Dstny, includes the following legal entities:

- Dstny for Service Provders AB
- Dstny Automate Ltd
- Dstny Analytics AB
- Dstny for Service Providers BV
- Dstny for Service Providers NV

2.2 Introduction

Dstny is a leading provider of as a service business communications applications to Service Providers. As a trusted partner, we understand the critical importance of security in the telecommunications industry. This white paper outlines our general security measures, policies, and procedures to ensure the protection of our customers' data and the uninterrupted delivery of our services.

The primary objectives of this white paper are to:

1. Provide an in-depth understanding of the general security measures implemented by Dstny.
2. Demonstrate our commitment to safeguarding customer data and maintaining the highest level of security in our operations.
3. Offer transparency to our service providers regarding our security practices and encourage confidence in our services.

Note that service specific security provisions are covered in the relevant service description and or service documentation.

2.3 Organizational Security

Ensuring a strong foundation of organizational security practices is vital to maintaining the overall security posture of Dstny. In this section, we delve into the key aspects of our organizational security.

2.3.1 Security Policies and Procedures

We have established comprehensive security policies and procedures that define the framework for security governance within Dstny. These policies cover areas such as information classification, acceptable use, incident response, and security awareness.

2.3.2 Security Roles and Responsibilities

To ensure clear accountability, we assign specific roles and responsibilities to personnel involved in security-related functions. This includes defining the responsibilities of the security team, system administrators, and employees across the organization.

2.3.3 Employee Awareness and Training

We recognize that employees play a crucial role in maintaining the security of our systems and data. We conduct regular security awareness training programs to educate employees about potential security risks, best practices, and their responsibilities in safeguarding sensitive information.

2.3.4 Human resource security

All personnel receive regular security awareness training and are informed about relevant security obligations, procedures, and their respective roles.

Employees are required to sign confidentiality/non-disclosure agreements as a condition of employment, and employment and criminal record background checks are performed (subject to local laws) as a condition of new employee hiring. Policies and procedures regarding corporate information security and data protection are enforced by the organization.

All employees and contractors who act on our behalf have a duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay.

We maintain a security posture characterized by the following human resource practices when employing personnel: All Personnel are party to confidentiality terms as part of the onboarding process and must regularly attest to compliance to the company's code of conduct.

2.3.5 Security Incident Response

We maintain a well-defined incident response framework to address security incidents promptly and effectively. This framework outlines the processes for reporting, assessing, containing, and recovering from security incidents.

2.3.6 Security Audits and Assessments

To continuously evaluate and improve our security posture, we conduct regular internal and external security audits and assessments. These audits help identify areas of improvement and ensure ongoing compliance with industry standards and regulations.

2.3.7 Third Party Risk Management

Third-Party Risk Management is essential for ensuring the security of our solution and protecting customer data. Hence we have established a robust vendor selection process and conduct thorough due diligence assessments. This includes evaluating the vendor's security practices, compliance with industry standards, and financial stability.

We include security requirements, responsibilities, and liabilities in contracts. The scope of the vendor's access to data and systems is be defined, and provisions for regular security assessments, compliance audits, and termination in case of breaches or non-compliance are in place, along with regular security assessments.

2.4 Physical Security

Physical security is a fundamental aspect of protecting our infrastructure and the sensitive data hosted within our facilities.

2.4.1 Access Controls

Our offices and data centers are equipped with robust access control mechanisms. Depending on the facility we employ pin enabled access cards and security personnel to restrict access to authorized individuals only. Access logs are maintained to track entry and exit.

2.4.2 Environmental Controls

To safeguard our infrastructure, we implement environmental controls, including fire suppression systems, temperature regulation, and humidity control. These measures help mitigate risks associated with fire, temperature fluctuations, and environmental hazards.

2.4.3 Redundancy and Backup Systems

To ensure the availability of our services, we deploy redundancy and backup systems in our data centers. This includes redundant power supplies, network connections, and backup generators. Regular testing and maintenance of these systems are conducted to ensure their effectiveness.

2.4.4 Data Center Security

All Dstny's data centres employ round-the-clock surveillance with interior and exterior cameras, as well as security guards who regularly patrol the premises. Access to the data centres is restricted and logged, with locked private cages and secure cabinets within these cages. Only authorized employees with specific roles are granted entry.

2.5 Access Management

Effective access management is essential to prevent unauthorized access to systems and data. In this section, we outline the measures implemented by Dstny to ensure secure access.

2.5.1 Authentication Mechanisms

We utilize industry-standard authentication mechanisms, such as username and password combinations, to verify user identities.

2.5.2 Authorization and Role-Based Access Controls (RBAC)

To manage access permissions effectively, we employ role-based access controls (RBAC). This allows us to assign specific privileges to users based on their job responsibilities, ensuring that they only have access to the resources required to perform their duties.

2.5.3 User Provisioning and Deprovisioning

To maintain secure access, we have well-defined processes for user provisioning and deprovisioning. These processes include verifying user requests, granting appropriate access privileges, and promptly revoking access when an individual's role or employment status changes.

2.5.4 Two-Factor Authentication (2FA) and Single Sign-On (SSO)

To enhance security and streamline user access, we employ two-factor authentication (2FA) as an additional security layer. Furthermore, we implement secure single sign-on (SSO) solutions that allow users to access multiple systems and applications using a single set of credentials.

2.5.5 Secure APIs and Interfaces

We secure our application programming interfaces (APIs) and interfaces used for customer interactions. This includes implementing authentication mechanisms, access controls, and encryption to ensure secure communication between our systems and those of our service providers.

2.6 Data Classification

We have a process of categorizing data based on its sensitivity, value, and criticality to our service providers and their customers. The process involves assigning labels or tags to data sets to indicate the level of protection and handling requirements the data require. Our purpose of data classification is to ensure that appropriate security controls and access restrictions are applied to different types of data, based on their importance and potential impact if compromised.

Our data classifications are:

1. **Public**: Data that is intended for public release and does not require any special protection measures. This may include marketing materials, public announcements, or general information that poses no risk if disclosed.
2. **Internal**: Data intended for internal use within our company but not publicly available. It may include internal communications, employee records, or non-sensitive operational data.
3. **Confidential**: Data that is sensitive and should be protected from unauthorized access. This may include personally identifiable information (PII), financial records, intellectual property, or sensitive customer information.

4. **Highly Confidential**: Data of the utmost sensitivity and criticality, requiring the highest level of protection. This may include trade secrets, classified information, or sensitive financial data.

2.7 Data Encryption

Protecting data in transit and at rest is paramount. In this section, we discuss the data encryption practices employed by Dstny.

2.7.1 Transport Layer Security (TLS)

We implement robust encryption protocols, such as Transport Layer Security (TLS), to secure data during transmission. TLS ensures secure communication between systems by encrypting data packets and providing integrity and authentication checks. We enforce a minimum level of TLS 1.2 in all relevant services.

2.7.2 Secure Real-Time Transport Protocol (SRTP)

For real-time communication sessions, such as voice and video calls, we employ the Secure Real-Time Transport Protocol (SRTP). SRTP provides end-to-end encryption and ensures the confidentiality and integrity of the transmitted media.

2.7.3 Encryption of Data at Rest

To protect data stored within our systems and databases, we employ encryption mechanisms. This includes encrypting sensitive data at rest using industry-standard encryption algorithms. Encryption keys are securely managed and protected to prevent unauthorized access.

Where public cloud infrastructure is used to host and provide our services, we employ the cloud provider's standard encryption mechanisms to protect data at rest, including the following:

- Data stored in databases
- Data stored within key vaults

- Data in storage queues

2.7.4 Key Management and Rotation

Effective key management is essential to ensure the security of encrypted data. Dstny follows industry best practices for key management, including secure storage, key rotation, and the use of strong cryptographic algorithms.

2.7.5 Compliance with Industry Standards and Regulations

We adhere to relevant industry standards and regulations, including but not limited to data encryption, such as the General Data Protection Regulation (GDPR) in the European Union and the UK. We recognize the importance of safeguarding our customers' data and strive to ensure its confidentiality, integrity, and availability. We have implemented robust internal controls and information security measures to protect sensitive data against unauthorized access, loss or disclosure.

2.8 Network Security

Securing our network infrastructure is critical to protecting our services and customer data. In this section, we outline the network security measures employed by Dstny.

2.8.1 Network Segmentation and Segregation

We implement network segmentation and segregation to isolate different network components and customer environments. This prevents unauthorized access and contains the impact of security breaches, reducing the risk of lateral movement across the network.

2.8.2 Firewalls

To protect our network from unauthorized access and potential threats, we deploy primary and secondary firewalls.

2.8.3 Network Monitoring and Logging

We maintain robust network monitoring and logging systems to capture network activities and detect anomalous behavior. Log data is regularly reviewed and analyzed to identify potential security incidents and aid in forensic investigations.

2.8.4 Fraud Prevention

We use fraud monitoring systems, destination blocking, and IP blocking in a multi-layered approach to fraud prevention. Fraud monitoring systems employ advanced algorithms to detect anomalies and patterns in real-time, enabling swift action against potential fraud. Destination blocking restricts transactions to high-risk regions, mitigating fraud risks. IP blocking blocks access from suspicious IP addresses, reducing fraudulent activities.

2.8.5 Secure Remote Access

For administrators and authorized users requiring remote access to our systems, we employ secure remote access mechanisms, such as virtual private networks (VPNs). These encrypted connections provide secure communication channels while ensuring the confidentiality of transmitted data.

2.8.6 Network Hardening

We follow industry best practices for network hardening, including disabling unnecessary services and protocols, implementing strong network access controls, and regularly updating and patching network devices and equipment.

2.9 Vulnerability Management

Proactively identifying and addressing security vulnerabilities is crucial in maintaining a robust security posture. In this section, we outline the vulnerability management practices implemented by Dstny.

2.9.1 Vulnerability Assessments

We conduct regular vulnerability assessments to identify potential weaknesses in our systems, networks, and applications. These assessments may include automated scanning tools, manual testing, and penetration testing performed by qualified security professionals.

2.9.2 Prioritization and Risk Management

Vulnerabilities identified during assessments are prioritized based on their severity and likelihood of exploitation. This allows us to allocate resources effectively for remediation, ensuring that critical vulnerabilities are addressed promptly.

2.9.3 Patching and Remediation

We maintain a comprehensive vulnerability management program, including timely patching and remediation. Patching involves applying security updates provided by software and hardware vendors to address known vulnerabilities. We have established processes to ensure the timely deployment of patches across our infrastructure.

2.9.4 Collaboration with Vendors

To address vulnerabilities effectively, we maintain strong relationships with all of the vendors involved in the delivery or our services. We collaborate with them to receive timely information about security patches, updates, and best practices. This collaboration helps us ensure the timely application of patches and the mitigation of potential risks.

2.10 Secure Development Lifecycle

Secure Development Lifecycle (SDL) We have implemented the Secure Development Lifecycle (SDL) framework developed by Microsoft to ensure the integration of security practices throughout our software development process. SDL prioritizes security at every stage, from design to maintenance, to deliver secure and reliable software solutions.

By adhering to SDL, we incorporate robust security measures throughout the development process. This includes conducting regular code reviews, threat modeling, and security testing to proactively identify and address vulnerabilities. Through these measures, we mitigate potential risks and significantly reduce the likelihood of security breaches.

Our commitment to SDL ensures that our software meets the highest security standards. We implement secure coding practices, conduct thorough security assessments, and adhere to industry-specific security regulations. This builds trust and confidence among our partners and customers, who can rely on our software to safeguard their data and maintain operational integrity.

Moreover, we prioritize ongoing security maintenance, staying vigilant about emerging threats and vulnerabilities. We provide timely updates and patches to address any identified security issues, ensuring the longevity and reliability of our software.

Overall, SDL plays a crucial role in enhancing the security and reliability of our services, providing long-term value and peace of mind to our customers.

2.11 Patch Management

Effective patch management is crucial in maintaining the security and stability of our systems. In this section, we detail the patch management practices implemented by Dstny.

2.11.1 Patch Deployment Process

We follow a systematic approach to patch management, encompassing the tracking, testing, and deployment of patches across our infrastructure and services. This process includes evaluating the impact of patches, testing them in controlled environments, and deploying them in production systems.

2.11.2 Patch Prioritization

Patches are prioritized based on their criticality, severity, and potential impact on our systems and services. Critical security patches addressing known vulnerabilities are given the highest priority and deployed urgently to mitigate risks.

2.11.3 Testing and Validation

Before deploying patches, we conduct rigorous testing and validation processes to minimize the risk of disruptions or compatibility issues. Patches are tested in controlled environments that closely resemble our production systems to ensure they do not introduce new vulnerabilities or conflicts.

2.11.4 Incident Response and Emergency Patching

In cases where critical vulnerabilities require immediate action, we have incident response procedures in place. These procedures outline the steps to be taken to address critical security issues promptly, including emergency patching to mitigate risks and prevent exploitation.

2.11.5 Patch Management Monitoring and Auditing

We maintain continuous monitoring and auditing of our patch management processes to ensure their effectiveness. This includes tracking patch deployment status, verifying compliance with patching policies, and conducting regular audits to identify areas for improvement.

2.12 Change Management

Change management plays a crucial role in maintaining a secure and stable environment. In this section, we outline the change management practices employed by Dstny.

2.12.1 Change Control Processes

We have well-defined change control processes and workflows in place to manage system configurations, software updates, and infrastructure modifications. These processes include thorough documentation, risk assessments, and approvals to ensure changes are implemented smoothly and securely.

2.12.2 Testing and Validation

All changes undergo rigorous testing and validation in controlled environments before being deployed to production systems. This helps identify any potential issues or conflicts and minimizes the risk of disruptions or security vulnerabilities.

2.12.3 Change Monitoring and Audit Trails

We maintain comprehensive change monitoring and audit trails to ensure accountability and traceability. This includes documenting the details of each change, capturing the approvals and actions taken, and keeping records of configuration changes made to systems and applications.

2.12.4 Change Advisory Board (CAB)

To ensure informed decision-making and effective change management, we have a Change Advisory Board (CAB) comprising key stakeholders from various departments. The CAB reviews proposed changes, assesses their potential impact, and provides recommendations and approvals.

2.12.5 Change Documentation and Communication

All changes are documented and communicated effectively within the organization. This includes providing clear instructions, documenting rollback plans, and ensuring relevant stakeholders are informed about the changes and their implications.

2.13 Threat Detection and Mitigation

Detecting and mitigating security threats is a continuous effort to ensure the safety of our systems and data. In this section, we discuss the threat detection and mitigation practices employed by Dstny.

2.13.1 Security Event Monitoring

We maintain security event monitoring systems that collect and analyze logs from various sources, such as network devices, servers, and applications. This helps us identify security incidents, correlate events, and respond promptly to potential threats.

2.13.2 Threat Intelligence Integration

We continuously monitor and integrate threat intelligence from trusted sources to enhance our security posture. This includes staying updated on the latest threat trends, emerging vulnerabilities, and new attack techniques. By leveraging threat intelligence, we can proactively identify and mitigate potential threats.

2.13.3 Incident Response and Forensic Investigation

In the event of a security incident, we have well-defined incident response procedures in place. These procedures outline the steps to be taken, including containment, eradication, recovery, and post-incident analysis. Forensic investigation techniques may be employed to gather evidence and understand the scope and impact of the incident.

2.14 Business Continuity and Disaster Recovery

Maintaining business continuity and having robust disaster recovery plans are critical for our operations. In this section, we discuss the measures implemented by Dstny to ensure uninterrupted service delivery.

2.14.1 Business Impact Analysis and Risk Assessments

We conduct comprehensive business impact analysis and risk assessments to identify potential vulnerabilities and prioritize critical systems and processes. This enables us to allocate resources effectively and implement appropriate measures for business continuity and disaster recovery.

2.14.2 Business Continuity Planning

We have well-defined business continuity plans in place, outlining the steps to be taken in the event of disruptions. These plans identify critical systems, define recovery time objectives (RTOs), and establish alternate processes to ensure minimal service disruption and quick recovery.

2.14.3 Redundancy and Failover Systems

To minimize single points of failure, we employ redundant systems and failover mechanisms. This includes redundant hardware, network connections, and data centers. These redundancies ensure high availability and quick failover in case of system or network failures.

2.14.4 Data Backup and Recovery

We maintain regular backups of critical data and implement robust data recovery procedures. These backups are securely stored and regularly tested to ensure their integrity and effectiveness in restoring systems and data in the event of data loss or system failures.

2.14.5 Testing and Exercising Business Continuity Plans

We conduct regular testing and exercising of our business continuity plans to validate their effectiveness and identify areas for improvement. These tests may include simulated disaster scenarios and recovery drills to assess the readiness and efficiency of our processes.

2.15 Logical Segregation and Multi-Tenancy Mode

Logical segregation and multi-tenancy mode are essential for maintaining the security and privacy of customer data. In this section, we explain the practices employed by Dstny in this regard.

2.15.1 Logical Segregation of Customer Data

We ensure logical segregation of customer data within our systems and databases. This includes using isolation techniques, such as separate database instances or virtualization, to prevent unauthorized access or data leakage between different customer environments.

2.15.2 Multi-Tenancy Mode

We employ multi-tenancy modes in our systems to efficiently serve multiple customers while maintaining data isolation and security. This mode allows for the secure sharing of resources, such as servers and storage, among multiple customers while ensuring strict segregation and access controls.

2.16 Account Security as a Shared Responsibility

Account security is a shared responsibility between Dstny, our service providers, and their customers. In this section, we highlight the importance of account security and outline the shared responsibilities.

2.16.1 User Account Management

It is a joint responsibility to ensure that the user account management systems we provide in our services are used effectively and according to design to maximize security.

2.16.2 Secure Communication Channels

We ensure that communication channels, such as customer portals and administrative interfaces, are secured using encryption protocols and strong access controls. This prevents unauthorized access and protects sensitive information transmitted between users and our systems.

2.16.3 Incident Reporting and Response

We encourage service providers and their customers to promptly report any suspected security incidents or breaches. We have established incident response procedures to investigate and mitigate such incidents, ensuring the timely resolution and prevention of future occurrences.

2.17 Conclusion

In conclusion, Dstny is dedicated to maintaining the highest level of security to protect our systems, customer data, and sensitive information. We have implemented a comprehensive security framework that encompasses network security, data encryption, access controls, incident response, and compliance with industry standards and regulations. By doing so, we strive to create a secure environment that instills trust and confidence in our customers.

We understand the evolving nature of cybersecurity threats and the need for continual improvement. As such, we regularly assess and update our security practices to stay ahead of emerging threats and ensure the effectiveness of our measures. We are committed to maintaining the confidentiality, integrity, and availability of our services, and we value the trust our customers place in us.

If you have any questions, concerns, or suggestions regarding our security practices, we invite you to reach out to us through your regular interface. Your feedback is valuable to us as we continually strive to enhance our security posture and address any potential vulnerabilities.

Together, we can create a secure and trusted environment for your business operations. Thank you for choosing Dstny, and we look forward to serving you with the highest level of security, privacy and reliability.

Dstny Security White Paper