Dalet Access Labs
WE MAKE TECHNOLOGY ACCESSIBLE

CORPORATE INFORMATION SECURITY MEASURES

LAST UPDATED: December 2024

CONTENTS

OVERVIEW

INTRODUCTION

This document describes the information security requirements and measures used to establish and enforce the corporate information security program at Dalet Access Labs Technology LLC and its affiliates (“**Dalet Access Labs**”).

Protecting data and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of Dalet Access Labs’s systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.

- Integrity – Integrity addresses the concern that data has not been modified or deleted in an unauthorized and undetected manner.

- Availability – Availability addresses ensuring timely and reliable access to and use of information.

SCOPE AND APPLICABILITY

The information security requirements and measures described in this document apply to Dalet Access Labs’s internal security with respect to our corporate network, applications, and systems.

SECURITY MANAGEMENT

INFORMATION SECURITY PROGRAM

Dalet Access Labs defines information security roles and responsibilities within its organization. Dalet Access Labs’s chief information security officer (“CISO”) oversees Dalet Access Labs’s information security (“ITSEC”) team dedicated to securing Dalet Access Labs’s corporate network, applications, and systems. Dalet Access Labs’s ITSEC team manages the corporate information security program. Dalet Access Labs’s corporate information security program aligns to ISO 27001, NIST SP 800-171, and NIST SP 800-53 r4.

INFORMATION SECURITY POLICIES

Dalet Access Labs maintains a written information security policy (as supplemented by additional internal standards, procedures, program, and guidelines) that defines employees’ responsibilities with respect to Dalet Access Labs’s corporate information security program. These policies and procedures are (i) evaluated and updated regularly, and (ii) made available to all Dalet Access Labs personnel.

INFORMATION SECURITY AWARENESS AND TRAINING

All Dalet Access Labs personnel undergo security awareness training during the initial onboarding process and then on an ongoing annual basis thereafter. Dalet Access Labs extends security awareness training to its subcontractors and other third-party service providers.

PERSONNEL SECURITY

Dalet Access Labs engages a reputable, commercially recognized background check or investigative entity to conduct background checks, as permitted by applicable law, on all new hires. Depending on the role, background checks may include criminal history checks, education verifications, employment verifications, and credit checks.

Dalet Access Labs ensures that all personnel enter into written non-disclosure/confidentiality

agreements. Dalet Access Labs has a disciplinary process in place for policy violations.

Dalet Access Labs promptly terminates personnel access to Dalet Access Labs’s corporate network and applications and computing resources when an individual leaves or discontinues work for Dalet Access Labs.

VENDOR RISK MANAGEMENT

When engaging third-party providers of products and services (“Vendors”) Dalet Access Labs requires non-disclosure agreements be in place with any potential Vendor before engaging in discussions regarding a potential business arrangement.

Dalet Access Labs's procurement and legal teams review proposed Vendor engagements. For those Vendors that will have access to Dalet Access Labs's internal networks and/or will store, process, or transmit data, Dalet Access Labs assesses the security and privacy practices of such Vendors to ensure they provide a level of security and privacy appropriate to the data and scope of services they are engaged to deliver.

Vendors are required to enter into appropriate security, confidentiality and privacy contract terms with Dalet Access Labs based on the risks presented by the Vendor assessment.

PHYSICAL SECURITY

OFFICES

Dalet Access Labs's facilities team is responsible for implementing physical and environmental security controls for office locations in accordance with Dalet Access Labs's access control and badging policy. Access to Dalet Access Labs offices is restricted to appropriate personnel and granted in accordance with the principle of least privilege and subject to monitoring measures. Employees, vendors, contractors, and visitors are expected to wear their badges in a clearly visible fashion at all times while on company property.

Dalet Access Labs partners with office building management to monitor access/egress points, including building main entrances and loading areas (if any).

DATA CENTERS

Dalet Access Labs does not operate any of its own data centers. Dalet Access Labs leverages third-party, industry-leading data center providers; these data center providers maintain extensive security controls, including secure design, access control, logging and monitoring, surveillance and detection, device management, and infrastructure maintenance.

INTERNAL ENVIRONMENT SECURITY

NETWORK ARCHITECTURE

Dalet Access Labs deploys firewalls to protect the perimeter of Dalet Access Labs's networks. Network traffic must pass through firewalls, which are monitored at all times. Dalet Access Labs has implemented and maintains an intrusion detection system to detect potential network compromises.

Dalet Access Labs engages a third-party firm to perform an annual penetration test on its internet perimeter network.

ACCESS CONTROL

Dalet Access Labs has implemented and maintains access controls mechanisms intended to prevent unauthorized access and limit access to users who have a business need to know in accordance with the principle of least privilege.

Dalet Access Labs uses role-based access control ("RBAC") based on predefined user accounts to ensure personnel only have access commensurate to their job function. Shared accounts are not permitted unless authorized by ITSEC executive management; if authorized, shared accounts are subject to additional security controls, documentation, and review.

Dalet Access Labs requires strong password control parameters (i.e., length, character complexity, and non-repeatability).

Dalet Access Labs leverages an access management program for provisioning (i.e., assigning, modifying, or revoking) user access for all systems and applications. All user accounts are approved by management prior to access permissions being granted. Access permissions are reviewed semi-annually. Dalet Access Labs revokes access to the corporate network, applications, and systems promptly after an individual ceases employment with Dalet Access Labs.

Access to Dalet Access Labs corporate applications (where commercially feasible) is controlled via Dalet Access Labs's SSO and requires authentication via the SSO platform.

Remote access requires multi-factor authentication and must employ Dalet Access Labs's VPN

solution. Dalet Access Labs personnel must comply with Dalet Access Labs's internal Acceptable Use

Policy.

ENDPOINT DEVICES

Dalet Access Labs personnel use endpoint devices configured with security software (i.e., antivirus, antimalware, encryption, etc.). Endpoint devices must (a) be configured for automatic patching; (b) be encrypted (i.e., full disk, endpoint encryption); (c) be secured with a protected (password) screen lock with the automatic activation feature; (d) be periodically scanned for restricted/prohibited software; (e) not be rooted or jailbroken; and (f) run an acceptable industry standard antimalware solution for which on-access scan and automatic update functionality is enabled.

To access Dalet Access Labs's corporate network, applications, and systems via personal mobile devices, Dalet Access Labs personnel must enroll in Dalet Access Labs's Mobile Device Management ("MDM") program. Dalet Access Labs's MDM program enforces minimum security requirements, including monitoring, remote wiping capability, encryption, and OS version updates.

OPERATIONAL SECURITY

ASSET MANAGEMENT

Dalet Access Labs maintains an inventory of assets and configurations via a centralized system.

CONFIGURATION MANAGEMENT

Dalet Access Labs's Change Advisory Board ("CAB") evaluates all corporate systems, applications, services, and capabilities prior to deployment in Dalet Access Labs's product networks. Dalet Access Labs maintains a repository of standard builds for operating systems used by Dalet Access Labs. Dalet Access Labs separates development and production environments to reduce the risks of unauthorized access and/or changes to the operational system or information.

LOGGING

Audit logging is enabled on Dalet Access Labs's corporate systems and applications; such audit logs are configured to capture sufficient detail (i.e., timestamp, event status, user details, etc.). All logs (where commercially feasible) are aggregated via Dalet Access Labs's SIEM platform, which is managed by the ITSEC team. Logs are retained for 365 days active / 365 archived.

VULNERABILITY MANAGEMENT

Dalet Access Labs runs internal and external network vulnerability scans on a regular basis. Identified vulnerabilities are remediated and/or mitigated in accordance with Dalet Access Labs's internal criticality SLA matrix; vulnerabilities identified and classified as critical risk are remediated or mitigated promptly after discovery.

COMMUNICATIONS MANAGEMENT

Dalet Access Labs encrypts data when transmitted electronically, including wirelessly, over any network other than the internal Dalet Access Labs network. Email transmissions are encrypted provided that the recipient supports TLS connections.

INCIDENT RESPONSE

Dalet Access Labs maintains an incident response program to identify, report and appropriately respond to known or suspected security incidents and/or personal data breaches.

Dalet Access Labs will investigate any security Incidents and/or personal data breaches of which Dalet Access Labs becomes aware and will define and execute an appropriate response plan. Customers may notify Dalet Access Labs of suspected vulnerability or incident by submitting a technical support case for Dalet Access Labs's evaluation.

Dalet Access Labs will notify customers of (a) security incidents as required by applicable law; and (b) personal data breaches without undue delay. Notification(s) of any security incident(s) or personal data breach(es) (as applicable) will be delivered to one or more of the customer's business, technical or administrative contacts by any means Dalet Access Labs selects, including via email. Dalet Access Labs in its sole discretion will provide timely information and reasonable cooperation in order for a customer to fulfill its data breach reporting obligations under applicable data protection laws. Dalet Access Labs will take such measures and actions as it considers necessary to remedy or mitigate the effects of a security incident or personal data breach.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Dalet Access Labs identifies requirements for and implements a business continuity management program to prevent catastrophic data loss and ensure timely restoration of corporate resources in the event of system failure, damage, or destruction. Business continuity and disaster recovery ("BC/DR") plans are established for all capabilities categorized as "P1 critical". Such BC/DR plans are reviewed quarterly and tested annually. Backups of P1 critical capabilities are retained for two years.