Declaration
Copyright of any content found in this document, including written descriptions, illustrations, methods and processes, all belong to DingTalk and it is protected by the relevant property rights and copyright laws. This document is to be used only for readers’ understanding of the security system of DingTalk. Without written authorization of DingTalk, no individual or institution is allowed to copy or quote any part of this Article in any way.

Version Change Record

<table>
<thead>
<tr>
<th>Time</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 15, 2016</td>
<td>V1.0</td>
<td>Version Creation</td>
</tr>
<tr>
<td>April 16, 2018</td>
<td>V2.0</td>
<td>Version Revision</td>
</tr>
</tbody>
</table>
Table of Contents

1 Preface .........................................................................................1
  1.1 Term Definitions .................................................................1

2 Security Culture ........................................................................3
  2.1 Security Organizations ......................................................3
  2.2 Philosophy on Talents .........................................................4
  2.3 Social Responsibility ............................................................5

3 Full-link Security Protection ...................................................6
  3.1 Client-side Security ..............................................................7
    3.1.1 Application Integrity ..................................................7
    3.1.2 Environmental Creditability .......................................7
    3.1.3 Data Confidentiality ...................................................8
    3.1.4 Account Security Risk Control .................................8
  3.2 Transmission Security ........................................................9
  3.3 Server-side Security ..........................................................9
    3.3.1 Application Security ..................................................9
    3.3.2 Database Security .....................................................11
    3.3.3 Middleware Security ...............................................12
  3.4 Infrastructure Security .......................................................12
    3.4.1 Physical Security .....................................................12
    3.4.2 Network security .....................................................14
    3.4.3 Host Security ..........................................................14
  3.5 Data Security .................................................................16
    3.5.1 Data Generation ......................................................16
    3.5.2 Data Transmission ..................................................16
    3.5.3 Data Usage ............................................................17
    3.5.4 Data Storage ..........................................................18
    3.5.5 Data Sharing ...........................................................18
    3.5.6 Data Destruction .....................................................19
    3.5.7 Data Security Audit ................................................19
  3.6 Security Operations ...........................................................19
3.6.1 Anti-intrusion ..................................................................................... 19
3.6.2 Red vs. Blue ...................................................................................... 20
3.6.3 Emergency Response ......................................................................... 20

4 Ecological Security .................................................................................... 22
4.1 Ecological Closed-loop .......................................................................... 22
4.2 Security Energizing .................................................................................. 23
4.3 Application Supervision .......................................................................... 23

5 Security Compliance ................................................................................... 24
5.1 System Construction .............................................................................. 24
5.2 Embracing Supervision .......................................................................... 24
5.3 Internal Control Auditing ....................................................................... 26
5.4 Integrity Compliance ............................................................................... 26

6 Summary ................................................................................................... 27
1 Preface

With the popularity of Mobile Internet, there are increased applications of instant messaging software. While technological innovations brings convenience to our lives and work, it also introduces many issues and hidden dangers such as security breaches relating to sensitive information, interference from irrelevant information and delay in message passing.

After its debut in 2015, DingTalk has grown into a Chinese smart mobile OA platform that provides a secure environment. Over the last three years, with its foundations stemming from its experience accumulated through the platforms operated by its partners: Taobao, Tmall and Alipay. In the last three years, Dingtalk has been innovating. With a continual usage of the system by more than 60,000 employees at Alibaba, a strong security system for mobile office ecosystem was established; one that provides 43 million middle and small-sized enterprises with “simple, efficient and safe” services.

To further elaborate on the above-mentioned enterprises’ perception on security of DingTalk, this document will prioritize four dimensions: security culture, full-link security protection, ecological security and security compliance. This document illustrates working concepts and practical methods of DingTalk while demonstrating Dingtalk’s pursuit of securing its users from Internet attacks, preventing user information leakage and its determination to protect lawful rights and interests of enterprises and citizens.

1.1 Term Definitions

**ASRC**: Alibaba Security Response Center.

**AES-256-GCM**: AES symmetric encryption algorithm; 256 is the intensity of the symmetric encryption algorithm while GCM (Galois/Counter Mode) means
the Counter mode with GMAC message authentication codes is employed in such a symmetric encryption.

**Alisql**: A branch of the official version MySQL. It applies to Alibaba Group businesses and Alibaba Cloud database services. Based on the community version, lots of improvements on performance and features were already made in this version.

**ChaCha20**: The encryption method of CHACHA20-POLY1305; a powerful new encryption algorithm.

**CloudDBA**: A smart database diagnostic optimization product developed by Alibaba itself; committed to becoming a database expert beside DBA, it provides self-service database diagnosis and optimization services.

**DSMM**: Data Security Maturity Model formulated under the leadership of Alibaba; it raises specific security requirements and metric systems on life cycle of data security on four dimensions, namely: organizational construction, man power, system process and technological tools.

**ECDH (Curve25519)**: Based on DH (Diffie-Hellman) key exchange algorithm of ECC (Elliptic Curve Cryptosystems, Elliptic Curvevea password system), exchanging parties can negotiate a secret key without sharing any secrets, among which Curve25519 is the algorithmic parameter.

**Full link**: The complete link for data interactions ranging from user side to server side.

**2FA**: Two-Factor Authentication, a secure method for password authentication.

**IDB**: Database management product developed by Alibaba itself; it integrates data management, structure management, diagnostic optimizations, real-time monitoring and system administration as a whole.

**LWS**: TLS1.3 encryption, secret key negotiation adopts the Elliptic Curve Cryptosystems ECDH (Curve25519) and the symmetric encryption algorithm
uses AES-256-GCM/Chacha20, which are adopted in a private secure communication protocol developed by Alibaba itself.

**SDL:** Security Development Lifecycle.

## 2 Security Culture

### 2.1 Security Organizations

Since DingTalk’s establishment, our organization has recognized the importance and strategic relevance in regards to information security and it's impact on the development and support to our business. Led by the CRO of Alibaba Group, we established a normative organizational structure for information security management and established up Security Management Committee consisting of team members from operational and product security.

In particular, members of the security product team mainly come from the Security Department of the Alibaba Group. Overall, they are responsible for developing, accessing, monitoring, enforcing, risk identifying, assessing and handling of the security products for the client side, the transmission and communication relating to the server side of DingTalk’s business. The Security Operation Team is composed mainly of individuals from the Security Department of the Alibaba Group and relevant staff from each of DingTalk’s product line. They are in charge of the operations relating to safety technique operations, compliance detection and conducting audit on businesses. Through their various capabilities in calculating, analysing, modeling and early detecting of potential operational risks to the business systems, they are able to optimize and enhance the overall security measures in regards to risks relating to the high volume of data processed through DingTalk.

In addition, in order to rapidly respond to businesses requests, the group at DingTalk has established an agile Scrum Team, which connects security capacity, such as safety techniques, security businesses, security ecosystem
and data security that are accumulated by the Security Department of the Alibaba Groups over the years. They reuses the full-link dynamic defense system of the Group to safeguard the stable and safe environment to use DingTalk and all of its strengths and business features. Furthermore, for special periods and select business needs, various work groups, such as the Evaluation Group on security architecture, the Governance Group on data privacy, the Special Tackling Group for application safety and the docker security group, were established to conduct cross-team coordination and communication, promptly responding to various business needs of DingTalk.

2.2 Philosophy on Talents

To aid in the safe operations of the Organization, Alibaba has established the following values: “Customers First, Team Work, Embracing Changes, Integrity, Passion and Dedication”, as well as a philosophy on talents: “Smart, Optimistic, Robust and Introspective” for its staff. Deriving from this philosophy, recruitment, onboarding, continuing education and resignation audit of DingTalk staff considers these key values. This ensures the management of security and its processes relating to employees is in line with requirements stipulated in the security policy of the Alibaba Group.

When recruiting and hiring employees, team leaders should consider carefully during examinations on the technical capacity of candidates at the phone or on-site interviews to ensure they meet the requirements for the position. After technical interviews, HR’s interview and background checks must also be made to ensure that moral characters and professional ethics of applicants meet our requirements. Next, employees must sign labor contracts and confidentiality agreements when onboarding. For staff of key positions and according to the sensitivity
level of the information they will handle, they will also need to sign special non-disclosure agreements separately. New employees should also attend training on standards of business conduct to acquaint themselves with the commitment alibaba groups made: that we will provide customers with justice, equity, security and reliability. At the same time, we’ll hold relevant trainings, such as Security of Data Permissions, Employees’ Conducts and Disciplines, and Red Lines on Security, to define our requirements and stipulations on security management, introduce responsibilities that individuals should perform in their daily work, as well as disciplinary measures they shall face when violating relevant security management requirements.

During the course of daily work, DingTalk staff can select to attend skill trainings which interest them independently via the online learning platform or offline special sharing sessions. At the same time, they also receive compulsory safety awareness trainings and examinations from the Organization, exam results and certifications of which shall be recorded and managed on platforms.

When employees resign their post or are transferred to other positions, HR and department heads should jointly determine the information assets to be recycled and application permissions to be closed. For key position staff, according to the circumstances, they should sign non-competition agreements and take a final resignation audit; for employees violating security management requirements, they shall be dealt with in accordance with disciplinary provisions and conventions for staff.

2.3 Social Responsibility

There are 43 million middle and small-sized enterprises in China. However, software service enterprises in the market only serve about 100,000 large-scale ones. Generally, investing social resources into serving a middle or
small-sized enterprise is of no cost performance at all, as middle and small-sized enterprises are scattered, bearing an average life cycle at about 2 years. Nevertheless, if we can aggregate the shared needs of such enterprises and craft a fair, transparent and high-efficient ecological sharing platform, all enterprises will be able to start from the same starting line, judging from multiple dimensions like utilization of social resources and a collaborative enterprise office.

To equalize social resources between large-scale enterprises and middle and small-sized ones and adhere to missions of Alibaba, which are to serve middle and small-sized enterprises and to facilitate making business anywhere, DingTalk provides such enterprises with a corporate collaborative office in a “simple, efficient, safe and happy” way. This is also the product original intention and social responsibility of DingTalk.

3 Full-link Security Protection

Guide by the “light control, heavy detection and fast response” policy of the Security Department of Alibaba Group, DingTalk fully embodies and mirrors all of the mature and time-tested security control measures implemented by the Alibaba Group in the server side, which includes multiple dimensions, such as PC sides, mobile sides, transmission pipelines and server sides. A complete in-depth defense system featuring dynamic prior control, real-time in-process defense and fast post response is built to ensure safety in use for DingTalk users.
3.1 Client-side Security

Reinforcing and strengthening four dimensions, namely, application integrity, environmental creditability, data confidentiality and account security risk control, DingTalk has safeguarded security of the client side effectively.

3.1.1 Application Integrity

Based on core technologies of Alibaba JAQ, DingTalk will apply security reinforcement measures, such as recompiling, shelling protection, instruction calling sequence modification and connect security components developed independently by Alibaba to applications before publishing. DingTalk client security has been safeguarded tremendously, when mobile security protection capacity of super APPs like Taobao and Alipay are copied instantly.

3.1.2 Environmental Creditability

With security measures like simulator detections, jailbreak and ROOT detections, anti-malware debugging and process injection detections, DingTalk provides safety measures for operating environments of applications.

Detection of simulator running: each time the program is woken DingTalk will detect if the application is running in a simulator.

Jailbreak and ROOT detections: each time the program is woken DingTalk will detect if the operating system of the terminal has been rooted.

Terminal process injection detection: when running, DingTalk will conduct dynamic monitoring to see if there are any abnormal processes loading in the operating environment of the user terminal.
Application sandbox environment is provided: both process space and data storage space of DingTalk will finish data encryption and decryption in the security sandbox.

Virus detection: users can select to use the QIANDUN virus scanning and removal feature provided by DingTalk to detect and remove viruses.

3.1.3 Data Confidentiality

For data information cached at client side, DingTalk employs a security sandbox and encryption solution to safeguard security of users’ data information. For enterprises with high information security requirements, third-party encryption services are also provided to realize secondary encryption on data information.

Security encryption: randomly generated secret keys that are bound to devices will be used when DingTalk encrypts and decrypts data. Even if the cracker managed to get encrypted data on user’s mobile phone, they cannot finish the decryption operation on their own phone. This practice has greatly ensured safety of data that is stored locally on the client side.

Security sandbox: the whole encryption and decryption processes of DingTalk in the client side are all finished in the security sandbox, revealing no secret key or encryption algorithm to the outside.

Security signature: based on the HMAC_SHA1 algorithm and specified keys, data will be attached to the signature, and as a result of such attachment, it can then be used to finish security validation on data transmitted.

3.1.4 Account Security Risk Control

Using an account security risk control system crafted by Alibaba, DingTalk can tag accounts and device risks, and trigger Two-factor verification as soon
as logins made from untrusted devices are detected. Meanwhile, with the account monitoring platform, abnormal behaviors like batch logins from the same device will be detected, warned or dealt with instantly by configuring the black list with a single click.

Apart from the existing account security risk control system, DingTalk also provides other extended account security control measures, like two-factor authentication (2FA), biometric identification and colleague relationship recognition, to provide user accounts with a safety guarantee with more dimensions.

3.2 Transmission Security

Based on SSL/TLS protocol, DingTalk has constructed a set of complete private secure communications protocol, LWS. With this private secure communications protocol, DingTalk’s end-to-end communication link encryption and signature are able to prevent eavesdropping and tampering, in order to ensure the security of transmission of data information.

3.3 Server-side Security

3.3.1 Application Security

Internet-oriented applications of Alibaba face at least millions of attacks each day. Based on the experience accumulated through these security responses, and by referring to industrial SDL practical experiences, the Security Department of Alibaba has formed a set of normative application security development life cycle management systems, fully covering all DingTalk businesses.
DingTalk SDL Flowchart

At the personnel training link, security engineers will provide developers with secure development specifications and security skill trainings by means of an online platform and offline security courses to improve developer’s awareness to safety concerns.

At security demand analysis link, depending on the feature requirement documents, such security demand shall be analyzed accordingly.

Communications on business scenarios, business processes and technical frameworks should also be made to form the suggestions after security demand analysis.

At the security development link, developing engineers must install the IDEA plug-in, developed by Alibaba, to realize coding normalization, security real-time detection and reminding, ensuring the coding is in line with Alibaba Java Developer's Handbook and requirements in relevant conventions on safe coding.

At the security test stage, black and white box scanning should be conducted via scanning tools developed by Alibaba. Combined with manual review on code defects and vulnerabilities, security risks identified by developers’ knowledge and skill, as well as business scenario logics, at each stage can thus be reduced.
At the project publishing stage, security engineers must finish a series of prior security checks, including code review, black-box and white-box testing on application systems. They should also check relevant test results and make sure all issues found are handled properly before such projects can be allowed online.

At the security operation and emergency response stage, with the SOC security operation platform, security engineers can analyze, handle, replay and track security events.

Based on data precipitated at each SDL stage, DingTalk has established quantitative analysis models, application security and monitoring systems thus, forming metrics maps on security development of each product line. Based on behavioral portraits of project teams and members at each stage, we supervise relevant staff and correct abnormal behaviors when they are identified. For example, failing to execute white-box scanning, publishing incorrectly with high-risk bugs or coding without passing security trainings. Ultimately, we can realize goals in which demanding personnel comprehends security, developers understand security, testing personnel knowledge on security and security personnel manages security. Consequently, quality of security coding for business systems can be improved to safeguard stable and safe operations to run applications.

3.3.2 Database Security

By customizing and optimizing mysql, Alibaba has developed Alisql. While performance is greatly improved, it also includes customization of features and service tailoring, providing powerful support for a stable operation of DingTalk databases. At the same time, for a safe, convenient and unified operation management of the databases, Alibaba developed a database management platform – iDB, to assist in unified authentication, permission
management, data change, database sheet synchronization and operation security audit, ensuring each SQL statement is in line with security requirements and performance specifications.

Additionally, the CloudDBA product developed by Alibaba provides DingTalk with systemic and professional database diagnosis and optimization capacity, enabling easy and overall diagnosis for troubleshooting items such as resource utilization, slow SQL, sessions/ events, locks, space, configurations and security, on database instances with one single click. Afterwards, a detailed diagnostic report and suggestions for optimizations will also be given.

3.3.3 Middleware Security

Middleware used in DingTalk server side employed a distributed permission system for identity verification and access control, safeguarding the confidentiality of sensitive information, such as data source and messages effectively.

3.4 Infrastructure Security

3.4.1 Physical Security

As for the management of the physical environment such as, temperature, humidity, electric forces and fire control, and the security during the operations of the data center, Dingtalk has selected the residing data center to be constructed or leased in strict accordance with A-classification requirements found in Design Specifications for Electronic Computer Machine Rooms (GB50174), Design Specifications for Special Telecom Rooms (YD5003-2014). Systems like air conditioners, electric power and fire control all adopted intelligent, high-stability and full redundancy designs. Furthermore,
in case there are any single-point equipment failure or abnormal events, alarms can be triggered automatically and a fast response can be initiated. As for access control management, applications accompanied by certificates of personal identity information must be filed out prior to accessing the data center. Visitors can only enter machine rooms after authorizations are obtained. In addition, their documents should be checked by security personnel at all times, and their access should be registered. Further, they should also be accompanied by the operator on duty. According to business significance and features, the interior of the data center is divided into different security zones, which consist of different access control systems. For zones with higher priority and requires increased security access, two-factor authentication like fingerprints are used. In addition, physical iron cages will be used for specific zones requiring higher security and isolation.

At the physical monitoring tour-inspection level, Alibaba established the GOC (Global Operations Center) to conduct real-time monitoring of the data centers. The GOC is tasked with handling any inaccuracies, failures and responses relating to the physical environments, equipment operation and traffic distribution, in order to achieve the digitization of operation metrics. Further, we also have a special team working 24/7. With regular automatic inspections for the online businesses and manual checks. In result, abnormal alerts can be located effectively, while handlers will then be notified in a timely and correct manner. We will also track the processing progress and review summaries periodically in order to ensure that the issues are fully resolved.

At the operations security management level, the IDC management team has established physical security guides and operational security management regulations for data centers. It also outlines base lines for physical and asset security inspections, conducts periodic security audits, checks rationality of
existing management measures and the effectiveness of executions and improves such practices continuously.

3.4.2 Network security

The overall network of Alibaba Group is mainly divided into ABTN and ACTN, among which ABTN is interconnected between egress routers of all data centers and operators, and a redundant and extended wide-area network is constructed via BGP protocol, while ACTN is the internal network Alibaba Group built for operation management and data synchronous interactions of each data center. To improve reliability and purity of business access, an abnormal flow cleaning platform will monitor and control access requests of Internet users flowing through external backbone network to realize a four to seven layer DDoS defense, clear machine behaviors and Web attack traffic, before access data reaches target servers.

A unified standardized network topology is established inside each data center, and different security zones are also divided. Based on importance of business supported by each zone, multiple security levels will be further divided. Stringent access control and routing policy are deployed between zones with different security levels. Meanwhile, flow DPI/DFI analysis and monitoring are realized with flow splitting, mirroring and sampling to identify abnormal behaviors efficiently.

3.4.3 Host Security

To enhance the host system security management of DingTalk businesses and comply with the “light control, heavy detection and fast response” policy of Alibaba Group for management and control mechanisms, Alibaba Group customized and optimized systemic components like Docker and Nginx, tailored all unnecessary services, minimized services and ports needed in
business activation and configured templates uniformly, intensifying self-
management and control to reduce possibility of vulnerability occurrences.
When accessing management, two-factor verification and authentication on
host logins are realized with AD domain integrated SSO and OTP of Alibaba
secure client side. Meanwhile, a network-layer access control policy and
virtual secure access groups are used to realize IP address and port based
security control. With automatic access control policy review tools, policy
compliance will be checked daily. Alarms will be sent via SMS, emails or
DingTalk messages immediately to ensure relevant personnel can handle it
instantly once any port information is wrongly opened.
As for the in-process detection mechanism, risk monitoring on abnormal
behaviors like abnormal system process, active outside connections, back-
door programs and system privilege escalations will be realized by deploying
intrusion detection agent on hosts; operation and maintenance staff of the
fortress machine will monitor operations and audit logs of target hosts to
realize multi-granular safety analysis and find potential risks in a timely
manner; besides, the software warehouse is scanned directly by mirror
vulnerability scanning tools periodically to ensure security and stability of
systemic components; fingerprint detection and recognition of base lines like
system services, port processes, software packages and traffic are realized
automatically with base line scanning tools every day to reveal potential
abnormal behaviors in a timely manner. For APT confrontations, a self-
developed agent covers office terminals and integrates services like deep
production servers, ensuring all-weather seamless collection of abnormal
actions. Additionally, multiple world-leading antivirus programs at the cloud
and a comprehensive scoring mechanism combining business scenarios and
multi-detection engines, under-reporting and false alarms can be reduced
effectively and the industry-leading APT detection service can thus be furnished.

For the post response mechanism, with the constantly iterated security algorithm model, abnormal behavior distributions of DingTalk business in cloud, pipelines and terminals, as well as characteristics of intrusions, will be computed to feed conversely and optimize defense strategy, realizing one-click hemostasis on known vulnerabilities, fast response to unknown vulnerabilities, searching and killing malicious files at the cloud, fast gray verification and update on system patches with ksplice.

3.5 Data Security

DingTalk strictly adheres to all security requirements of DSMM and implants all matured security control measures of Alibaba Group during each stage of the data’s life cycle, from generation, storage, usage, transmission, sharing and destruction, to ensuring confidentiality, integrity and reliability of user data.

3.5.1 Data Generation

When drafting data security policy specifications, according to relevant attributes like data type, sensitivity and data value, DingTalk has defined data classification and grading standards. When data is generated, it will be tagged with such classification and grading uniformly, to ensure that classified management and control, as well as classified authorization, will be applied to all data by following the policy specification.

3.5.2 Data Transmission

All public-facing DingTalk applications must be connected to the unified application gateway to realize TLS encryption and unified credential
management to ensure whole-site https secure access; for internal-facing businesses involving signature authentication or encryption, access must be done through encryption machines uniformly, through API different signatures, authentication and encryption of various applications can be realized with data interconnections. Secret keys are prevented from leaving encryption machines, confidentiality, integrity, availability and nonrepudiation of data are also assured.

3.5.3 Data Usage

For DingTalk's front-end applications, all sensitive pages will be attached with digital watermarks and, by default, sensitive information is hidden and displayed as dots. For server side applications, they must be accessed with management system permission uniformly, while based on their permissions, roles and risk levels, accessing subjects must file applications as required and explain in detail all relevant information, such as content, reason and duration of the accessing attempt. Granted access permissions should also be reviewed periodically, and such permissions should be closed automatically after the staff transferred to another position or has resigned; for database operations, all operation commands regarding adding, deleting and modifying will be monitored the whole time, all action logs will be stored centrally and real-time analysis will be applied in all operations flow. When behaviors violating security management requirements, such as high-risk sql statements, batch non-compliant operations and abnormal operations in dangerous periods, are identified, alerts will be sent promptly and real-time online interception can be applied.
3.5.4 Data Storage

From the client side, AES-256-GCM, a high-strength symmetric key algorithm, is adopted for users' chat messages (including texts, images, audio, video and other files) to encrypt and protect the entire database. Based on users’ credible device information, a unique secret key can also be generated to protect sensitive data stored in the client side from being acquired illegally by attackers. Meanwhile, enterprises can set up automatic destruction on users' chat messages to ensure confidentiality of local data.

For the server side, each application there uses an independent key. A high-strength symmetric key algorithm, AES-256-GCM, is also used to encrypt data. As each enterprise holds a different secret key that is managed by a hardware encryption system uniformly, security of data storage at server side is guaranteed.

3.5.5 Data Sharing

Regarding opening data to the outside world for sharing, DingTalk shall strictly follow the requirements of the Cyber Security Law. Taking safeguarding users’ privacy information as the primary premise, it has formulated detailed rules and regulations governing disclosing data externally and established the following principles to be followed for such outputs:

Protecting users’ privacy: without full authorization, data regarding users’ privacy cannot be collected, analyzed or output to any third party.

Necessity and minimization: for external data output, its scope, volume and the number of informed persons must be minimized, except in the cases where the public needs to be notified of such output data as required by law.

Compliance: for external data cooperation, requirements like laws, regulations, policies and industrial standards, which are applicable to Alibaba Group, must be followed.
3.5.6 Data Destruction

For information processing facilities and data purging, disk demagnetization and physical destruction should be conducted on storage mediums by following DoD 5220.22-M and NIST 800-88 standards to prevent data leakage risks before they are moved out of data centers.

3.5.7 Data Security Audit

During the data life cycle, DingTalk has established a full-link risk detection and perception system to conduct real-time detection and analysis on abnormal data access records by contextual analysis, behavior filtration and experts’ operations. Once abnormal behaviors, such as login failures, permission escalations, illegal accesses and downloading of sensitive data, are detected, alarms will be sounded in a timely manner to ensure that such violation operations are traceable.

3.6 Security Operations

3.6.1 Anti-intrusion

DingTalk businesses generate massive logs of data every day. Data includes information like terminal behavior logs, network security logs, system running and intrusion detection logs, WAF protection logs, network flow and base line inspections. Based on such logs, with the assistance of big data security analysis platform and assisted by rules like pattern matching, sandbox analysis, machine learning and experts’ experience, Alibaba can extract objectives-oriented situational data to establish portraits of users’ behaviors, realize automatic identification, analysis and correlation of abnormal behavior data, restore attack paths, tag full-link risks, score comprehensive evaluations, perceive potential risks and specific APT attacks precisely and
effectively. Combined with the abnormal flow cleaning platform, a one-click handling can be realized to safeguard security of business systems and privacy of clients’ data.

3.6.2 Red vs. Blue

In regards to attacks, independent attacks against the defense drill team assembled by the Security Department of Alibaba will fully review attack paths and conduct organized penetration test work. At the same time, an attack against the defense drill platform with built-in historical attacking data, vulnerability library, basic asset information and experts’ experience is established, on which an attack against the defense drill will be performed each day and a full-link drill is conducted each month. In addition, ASRC white caps are invited to perform security crowd-testing periodically. During such continuous confrontations, security vulnerabilities in various business systems of Alibaba will be revealed quickly, efficiently and fully. When business rectifications are being advanced, attack characteristics can be precipitated, security detection and protection control policy can also be optimized to safeguard safe and stabilize operations of business systems.

3.6.3 Emergency Response

With a unified security event emergency response platform, Alibaba can archive a closed-loop management, like discovering, handling, tracing and replaying security events, and continue its operations. Its emergency management level on unforeseen security events can be completely improved, and safe and stable operations of business systems can thus be assured.

At the security event discovering stage, via OpenAPI, this Platform can be connected to platforms like white-box and black-box scanning products, threat
intelligence systems and ASRC, as well as asset management systems, to conduct real-time collections of relevant domain names and IP information about security events. Based on such information, event details will be automatically forwarded to relevant security emergency response experts. At the security event handling stage, security emergency response experts will carry out a 24/7 real-time response. Once they receive SMS, emails or DingTalk message alerts, they will confirm, within the prescribed time, information such as if such security events are false alarms, its scope of influence and risk levels. Once a false alarm is confirmed, processes will be terminated. If it is confirmed it is a known type of security event, existing solutions will be connected, and processes will be passed on to development engineers and operation and maintenance engineers who are responsible for the businesses affected. If an unknown type of security event is confirmed, security emergency response experts will coordinate personnel for security research, product defense and attack-defense to extract characteristics of such events, formulate temporary hemostasis measures, strengthen monitoring on flow and behaviors, define safe solutions and assist business parties in their rectifications.

At the security event tracing stage, the Traceability and Forensics Team will collect activity logs of business terminals, pipelines and cloud affected as required, conduct a comprehensive analysis, fully restore generating process of such security events and perform targeted rectifications and reinforcements. If needed, they shall also cooperate with public security organs in case-filling and handling.

At the security event replaying stage, based on information like event type, event ranking and business distributions, operators on security event emergency management platform shall regularly organize the staff to conduct a case study, summarize and analyze primary causes of such events, so that
prior control and in-process defense mechanisms and processes can be improved.

4 Ecological Security

4.1 Ecological Closed-loop

With security terminal containers, private safe encryption channels and security cloud containers, DingTalk provides ISV with an efficient, flexible, safe and integrated solution. When access speed is assured, stability of micro applications can be greatly improved, and hijacks can also be prevented effectively.

Aiming at high-risk business hazards, such as data leakage and brute download, in the application store, DingTalk applies special administration and continuous monitoring and audit. This constantly improves its security solutions at terminals, pipelines and cloud and reinforces the security control on ISV persistently, protects user data from leaks, and ensures security, stability and efficiency of applications provided by ISV.
4.2 Security Energizing

DingTalk ecological security has established review processes and standards for third party applications to go online. By publishing ISV access requirement and security development specifications for languages like PHP, JAVA and H5, DingTalk is literally assembling and cultivating security teams for third-party ISV and enterprise developers in the way of cooperative partnerships, providing DingTalk application store developers and enterprises with security assurance capabilities.

4.3 Application Supervision

Before micro applications are published in application store, developers need to submit security test reports first, which will then be reviewed by DingTalk security experts. Such applications can only be allowed to go online after the acceptance inspections are passed. After such micro applications are published, in accordance with DingTalk’s specification requirements, developers shall authorize DingTalk security experts to make security assessments. Micro applications will be attached the safety certificate labels if their conformities with specification requirements of DingTalk are confirmed. Furthermore, for micro applications published by third-party developers, DingTalk will monitor exceptional cases in the application store and conduct security scanning to locate applications with possible security vulnerabilities, violations or non-conformities in a timely manner, in order that a green and credible DingTalk open platform can be built.
5 Security Compliance

5.1 System Construction

In accordance with requirements found in Cyber Security Law of the People's Republic of China, by referring to domestic and overseas standards and best practices including ISO27001, ISO27018, PCI DSS, SOC 2/3, GDPR, TrustE and information security level protection, and combined with years of Internet security work experience of Alibaba Group, DingTalk has established a security system covering 14 control domains, including security tactical policy, organizational and personnel security, development security, operation security, outsourcing security, business continuity of information security, and compliance audit. For each control domain, a normative four-layer document architecture and a configurable metrics system are established. Basically, all security processes are fundamentally online, process data has turned into indexes, operation metrics has turned to a platform, and all security control measures of DingTalk have been covered, assuring security, stability and compliance of DingTalk effectively.

5.2 Embracing Supervision

Guided by the “light control, heavy detection and fast response” policy of the Security Department of Alibaba Group, DingTalk carries out security compliance certification work actively. So far, it has won and passed the following certification approvals:

**Classified Protection of Information Security**: this is a national information system level certification supervised by the Ministry of Public Security of the People's Republic of China, approved and issued by the local public security organs. In 2016, the Ministry of Public Security organized many national
teams to conduct level evaluations, risk assessment and penetration tests on the information system of DingTalk. Several academicians of the Chinese Academy of Sciences and the Chinese Academy of Engineering, as well as industrial security experts, reviewed such assessment results and confirmed the security level of DingTalk information system is “Level Three”, proving that security control measures of DingTalk are in accordance with national requirements.

**ISO/IEC 27001**: ISO27001:2013 Information Security Management System is the most widely used information security management standard in the world. DingTalk is the first Chinese mobile cooperative office platform service provider that has been certified with the ISO27001:2013 certification, based on which the DingTalk Information Security Management System (ISMS) is established to cover a full life cycle, like product development, business operation, security assurance and marketing promotion. Confidentiality, integrity and availability of DingTalk businesses and data can be safeguarded effectively and persistently when each “person in charge” follows clear “specifications” and standard “processes”, and outputs valid “record sheets” of processes.

**ISO/IEC 27018**: ISO/IEC27018:2014 is the first cloud privacy protecting standard set by the International Organization for Standardization. It emphasizes that collection, usage and storage of data must be authorized by users, and users should possess full control power and reasonable transparency on their data stored.

**SOCII Security Auditing Report**: SOC report refers to Report on System and Organization Controls. Content framework and format of such reports are formulated by the American Institute of Certified Public Accountants (AICPA). Such reports place emphasis on service control that are related to security of enterprises, integrity of processes, availability, confidentiality and privacy.
With the Three Level classified protection certification supervised by the Ministry of Public Security, ISO27001:2013 Information Security Management System certification, ISO27018 user privacy certification under public cloud systems and SOCⅡ type I security auditing report issued by PricewaterhouseCoopers, a world-renowned accounting firm, it indicates that the security practices of DingTalk have met the domestic leading and world first-class security standard requirements. It further implies that when using DingTalk, confidentiality, integrity, availability and privacy of user data have aligned with the best practice both at home and aboard, and such endeavors have finished security authenticated and audit by an independent third party.

5.3 Internal Control Auditing

With the rapid development of DingTalk businesses, technological changes introduced by the business innovations have made internal control compliance a challenging task. Consequently, according to security management requirements and security metrics system practices of Alibaba Group, DingTalk periodically invites security compliance teams of the Group to quantitative and qualitative risk assessments and security auditing on rationality of DingTalk’s security management and effectiveness of its security control measures, pursues security policy requirements of the Group entirety, reveal potential security compliance risks timely, improves security levels and perfects the security system continuously.

5.4 Integrity Compliance

Once any abnormal behaviors such as leaks of users’ privacy, malicious tampering of user data and unauthorized execution of rule-breaking operations are identified when performing DingTalk daily businesses, the Integrity Compliance Department shall conduct a security compliance audit by
following security rules and regulations like the Standards of Business Conduct, Employee Discipline Regulations and Red Lines on Security. According to the circumstances, it will then impose punishments properly. For severe cases, violators will be imposed a dishonorable discharge, while for extremely severe violations we reserve the right to hold such violators accountable for civil or criminal liabilities.

6 Summary

Guided by the “light control, heavy detection and fast response” policy of the Security Department of Alibaba Group, DingTalk shall employ technical innovations and big data operations to improve each security control measure continuously, explore and research leading technologies like automatic analysis and exploration on vulnerabilities, homomorphic encryption and differential privacy to reinforce the security system construction, embrace security supervision at all levels both at home and abroad actively, and standardize internal security operations. However, some risks still exist, especially with such a complex Internet situation. DingTalk faces severe tests each day when its internal businesses are being iterated and external attacks are emerging in an endless stream. To safeguard safety of each DingTalk user effectively, supported by powerful resources of the Alibaba Group, each DingTalk staff shall carry this cause forward with constant persistence and detailed attention.