

# Independent Assessor's Transmittal Letter on Twitter's Information Security Program

For the Period September 13, 2019 to September 12, 2021  
With Report of Independent Accountants



## Table of Contents

Transmittal Letter .....	1
EY’s Security Assessment Approach .....	2
Independence .....	2
EY Assessment Process Overview .....	3
EY’s Assessment of Part III A – D of the Decision and Order (the “Order”) .....	6
A. Set forth the specific administrative, technical, and physical safeguards that Twitter has implemented and maintained during the reporting period. ....	6
B. Explain how such safeguards are appropriate to Twitter’s size and complexity, the nature and scope of its activities, and the sensitivity of the non-public consumer information collected from or about consumers. ....	6
C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of the Order. ....	7
D. Certify that Twitter’s security program is operating with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information and that the program has so operated throughout the reporting period .....	18
Addendum to Transmittal Letter .....	19
Company Overview .....	19
EY’s Assessment of Twitter’s Security Program .....	20
Information Security Program Assessment .....	20
Twitter Information Security Program Governance .....	20
Twitter Information Security Program Scope .....	21
Report of Independent Accountants .....	24
Exhibit I – Management’s Assertion .....	26
Attachment A: .....	27
Twitter’s Information Security Program Criteria, Supporting Controls, Test Procedures, and Assessment Results .....	27
Attachment B: .....	84
Assessment Interviews Summary .....	84



Ernst & Young LLP  
Suite 1600  
560 Mission Street  
San Francisco, CA  
94104-2907

Tel: +1 415 894 8000  
Fax: +1 415 894 8099

Mr. Sean Edgett  
General Counsel  
Twitter, Inc.  
1355 Market Street  
San Francisco, CA 94103

## Transmittal Letter

Dear Mr. Edgett,

We are issuing the attached Report of Independent Accountants (“Report”) on Twitter, Inc.’s (“Twitter’s” or “the Company’s”) Management Assertion (“Assertion”) in connection with our examination to determine whether, for the two years ending September 12, 2021 (the “Reporting Period”), in accordance with Parts II and III of the Decision and Order (the “Order”) issued on March 2, 2011 by the U.S. Federal Trade Commission (“FTC”):

- The Company established and implemented a comprehensive information security program (“Twitter Information Security Program” or “Subject Matter”) based on the Internal Organization for Standardization (“ISO”) / International Electrotechnical Commission (“IEC”) Standard 27002:2013 (“ISO/IEC 27002:2013”).
- The Company conducted a risk assessment to identify material risks, both internal and external, and assessed the sufficiency of the safeguards in place to control those risks which could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of non-public consumer information or in unauthorized administrative control of the Twitter system.
- The Company’s administrative, technical, and physical safeguards within the Twitter Information Security Program are appropriate to its size and complexity, the nature and scope of Twitter’s activities, and the sensitivity of non-public consumer information collected from consumers.
- The Company’s security controls meet or exceed the protections required by Part II of the Order.
- The Twitter Information Security Program operated with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of non-public consumer information (as defined by the Order), and the program has so operated throughout the reporting period.

This letter should be read in conjunction with the Report.

Part II of the Order requires Twitter to “establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of non-public consumer information.” Part III of the Order requires Twitter to obtain biennial assessments (“Assessments”) of its Twitter Information Security Program from a “qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession.” Twitter retained Ernst & Young LLP (“EY”) to perform the Assessment for the Reporting Period.

## EY's Security Assessment Approach

Part III of the Order requires that the Assessments be performed by "a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession." This report was issued by EY under applicable professional standards that meet these requirements.

EY, an American Institute of Certified Public Accountants ("AICPA") member firm, must comply with the public accounting profession's technical and ethical standards, including the AICPA's Code of Professional Conduct. In addition to the Code of Professional Conduct, the AICPA publishes standards, which delineate specific requirements Certified Public Accountants are consistently required to follow in the course of engagements.

One such standard, the Concepts Common to All Attestation Engagements (AT-C Section 105), states that practitioners must meet specific requirements to accept and perform assessments, such as the following:

### Assignment of the Engagement Team and the Practitioner's Specialists:

The engagement partner should be satisfied that:

- a. the engagement team, and any of practitioner's external specialists, collectively, have the appropriate competence, including knowledge of the subject matter, and capabilities to:
  - a. perform the engagement in accordance with the professional standards and applicable legal and regulatory requirements; and
  - b. enable the issuance of a practitioner's report that is appropriate in the circumstances.

Furthermore, "[t]he responsible party in an attestation engagement must have a reasonable basis for measuring or evaluating the subject matter."

EY complied with all these standards in performing the assessment. Furthermore, all EY personnel directing the examination were sufficiently qualified. All EY personnel directing the examination and preparing the Report have technical and business knowledge and experience in the field of cybersecurity and privacy.

### Independence

AICPA standards also require EY to maintain independence in the performance of audit and examination engagements. The AICPA standard states, "[a] member in public practice shall be independent in the performance of professional services as required by standards promulgated by bodies designed by Council." (See AICPA Code of Professional Code sec 1.200 Independence.) The standard states that to determine whether an auditor has the requisite independence in the performance of professional services, an AICPA member

“should evaluate whether the relationship or circumstances would lead a reasonable and informed third party who is aware of the relevant information to conclude that there is a threat to either the member’s or the firm’s independence, or both, that is not at an acceptable level.”

Independence is comprised of independence of mind and in appearance, both of which are required of the AICPA member firm and the auditors engaged in the professional service. Independence of mind requires that the member maintain a state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and skepticism. Independence of appearance is achieved by the avoidance of facts and circumstances that are so significant that a reasonable and informed third party would likely conclude, weighing all the specific facts and circumstances, that a firm’s, or a member of the firm’s audit team’s, integrity, objectivity, or professional skepticism has been compromised.

EY is independent in accordance with the AICPA standards required for this engagement.

#### **EY Assessment Process Overview**

The procedures performed by EY were designed to:

- Examine the Assertion concerning Twitter’s compliance with Part II of the Order, stating that Twitter has established and implemented the Subject Matter to meet the requirements of the Order based on the Criteria and supporting controls;
- Determine that the controls were implemented and maintained by Twitter to address the Criteria; and
- Determine the operating effectiveness of the controls during the Reporting Period based on the Criteria.

EY conducted testing procedures to determine that the controls were implemented, maintained, and operated effectively by Twitter during the Reporting Period. The nature of EY’s testing was dependent on each control, and EY developed our test procedures based on our understanding of the risk, complexity, and other factors. EY used a combination of inquiry, observation, and inspection to test the controls. Refer below for a description of the test procedures utilized by EY:

Inquiry: EY held discussions with Twitter personnel to obtain an understanding of the Subject Matter and its objectives, in order to understand the controls implemented by Twitter and how they operate to meet or exceed the protections required by the Order. Twitter personnel included individuals from various departments, a listing of which is included in *Attachment B: Assessment Interviews Summary*. The inquiry procedures included asking Twitter personnel about Twitter’s controls, policies, and procedures relevant to their positions, as well as their roles and responsibilities. To validate the information obtained in the discussions, EY performed corroborative inquiry procedures with multiple individuals and, using the testing techniques below, obtained and inspected

evidence to validate the responses. When EY performed corroborative inquiry, EY asked several people across Twitter about a given control or situation. EY does not rely on inquiry procedures alone, but rather combines inquiry procedures with additional forms of testing (e.g., observation or inspection) to evaluate and reach conclusions on the effectiveness of the controls.

Observation: EY utilizes the observation testing method to determine that the controls were implemented, maintained, and operated effectively. EY met with relevant Twitter personnel and observed how the controls were designed and functioned, to determine whether Twitter has implemented controls that meet or exceed the Criteria.

Examination or Inspection of Evidence: EY used the examination or inspection testing method to validate the operating effectiveness of the controls and to evaluate the sufficiency of the controls implemented to meet or exceed the Criteria on which the Assertion is based. EY inspected, either physically or online, information, configurations, and documents (including documentation of Twitter's policies and procedures, risk assessment, and training and awareness programs) to evaluate the operating effectiveness of the controls and safeguards implemented by Twitter. The nature of the evidence examined varied from control to control and, where appropriate, other testing procedures, such as observation and inquiry, were utilized to confirm the results of the examination procedures.

EY performed walkthroughs of the processes and controls to determine whether the controls were built to achieve the Criteria on which the Assertion is based, as well as to determine whether the controls had been placed into operation. To perform a walkthrough, EY met with relevant Twitter control owners and interviewed them regarding how Twitter implemented the controls. Additionally, EY assessed whether the individuals performing the controls possessed the necessary authority and competence to operate the controls effectively. Our test procedures included performing a combination of inquiry, observation, and inspection techniques.

To assess operating effectiveness, EY performed procedures to determine whether the controls were executed by Twitter (or Twitter's system, if automated) at the appropriate frequency, and whether documentation and support were maintained to demonstrate the controls' execution. Our operating effectiveness test procedures included, where appropriate, selecting samples from populations appropriate for the Reporting Period and performing a combination of inquiry, observation, and/or inspection procedures to evaluate the effectiveness of the controls documented in *Attachment A: Twitter's Information Security Program Criteria, Supporting Controls, Test Procedures, and Assessment Results*.

Over the course of the Reporting Period, EY performed procedures that included interviewing individuals from several departments within Twitter. (Please see *Attachment B: Assessment Interviews Summary* for individuals interviewed as part of the Assessment.) Additionally, EY conducted periodic Security Assessor Briefings with Twitter, during which Twitter provided EY

with relevant updates from Twitter's Security Team regarding recent security vulnerabilities and remediation strategies. During these meetings, Twitter's team discussed: (1) breaches or potential breaches that could impact the Subject Matter including the operating effectiveness of Twitter's Information Security Program controls, and (2) Twitter's interactions with regulators regarding topics that may be relevant to Twitter's assertions or Information Security Program controls during the Reporting Period. Following each Security Assessor Briefing, EY evaluated the information shared, to determine whether such updates required modifications to our test procedures or required Twitter to provide additional documentation to support our procedures. Please see *Addendum to Transmittal Letter* for more information on EY's review of Twitter's Information Security Program.

During the Reporting Period, a global pandemic was declared, due to the spread of the COVID-19 virus. The global pandemic resulted in federal, state, and local orders that impacted organizations in a number of ways, including the shift of all non-essential personnel to work from home beginning mid-March 2020. However, this did not impact EY's ability to conduct our procedures or complete our examination. In addition, EY conducted inquiries with Twitter to assess the possible impact of the pandemic on the Subject Matter, including Twitter's risk assessment and supporting controls. Based on our inquiries, there were no significant changes to the Subject Matter as a result of the pandemic.

**EY: Confidential Information**

*Ernst & Young LLP*

11 November 2021

## **EY's Assessment of Part III A - D of the Decision and Order (the "Order")**

*Attachment A: Twitter's Information Security Program Criteria, Supporting Controls, Test Procedures, and Assessment Results* sets forth tables that describe the scope of Twitter's Information Security Program subject to this Assessment. Twitter based its Information Security Program on the ISO/IEC 27002:2013 and additional Twitter-specific criteria in order to meet or exceed the protections required under Part II of the Order. The section below documents EY's assessment results. EY's final conclusions on the Assertion are detailed in the Report.

**A. Set forth the specific administrative, technical, and physical safeguards that Twitter has implemented and maintained during the reporting period.**

As detailed within *Attachment A: Twitter's Information Security Program Criteria, Supporting Controls, Test Procedures, and Assessment Results*, Twitter has listed the controls that were implemented and maintained during the Reporting Period. Our procedures, as defined in the section entitled, "EY Assessment Process Overview," support the results of our assessment that the controls have been implemented and maintained during the Reporting Period.

**B. Explain how such safeguards are appropriate to Twitter's size and complexity, the nature and scope of its activities, and the sensitivity of the non-public consumer information collected from or about consumers.**

Based on the size and complexity, the nature and scope of Twitter's activities, and the sensitivity of the personal information collected from, or about, Consumers, Twitter's management developed the Criteria and supporting controls detailed in *Attachment A: Twitter's Information Security Program Criteria, Supporting Controls, Test Procedures, and Assessment Results* as the basis for its Information Security Program. The Criteria and supporting controls were evaluated against the AICPA standards for suitable and available criteria (AT-C 105.A42), which requires criteria to be:

- (1) Relevant to the subject matter
- (2) Objective and free from bias
- (3) Consistently measurable using qualitative or quantitative attributes
- (4) Complete and not missing any factors that could reasonably be expected to affect decisions of the intended users, which are made on the basis of that subject matter

Upon evaluation of the Criteria, EY confirmed that the Criteria were relevant, objective, measurable, and complete to address the risks identified by Twitter's security risk assessment in each of the areas defined by the Assertion. Therefore, the Criteria are appropriate for Twitter's size and complexity, the nature and scope of Twitter's activities, and the sensitivity of non-public consumer information collected from or about consumers.



C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of the Order.

## Twitter: Information Security Plan Details

Through the establishment and implementation of this Information Security Program, Twitter has implemented the following protections:

1. Designation of an employee or employees to coordinate and be accountable for the information security program.

## Twitter: Information Security Plan Details

# Twitter: Information Security Plan Details

2. Identification of reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of nonpublic consumer information or in unauthorized administrative control of the Twitter system, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, account takeovers, or other systems failures.

# Twitter: Information Security Plan Details

## Twitter: Information Security Plan Details

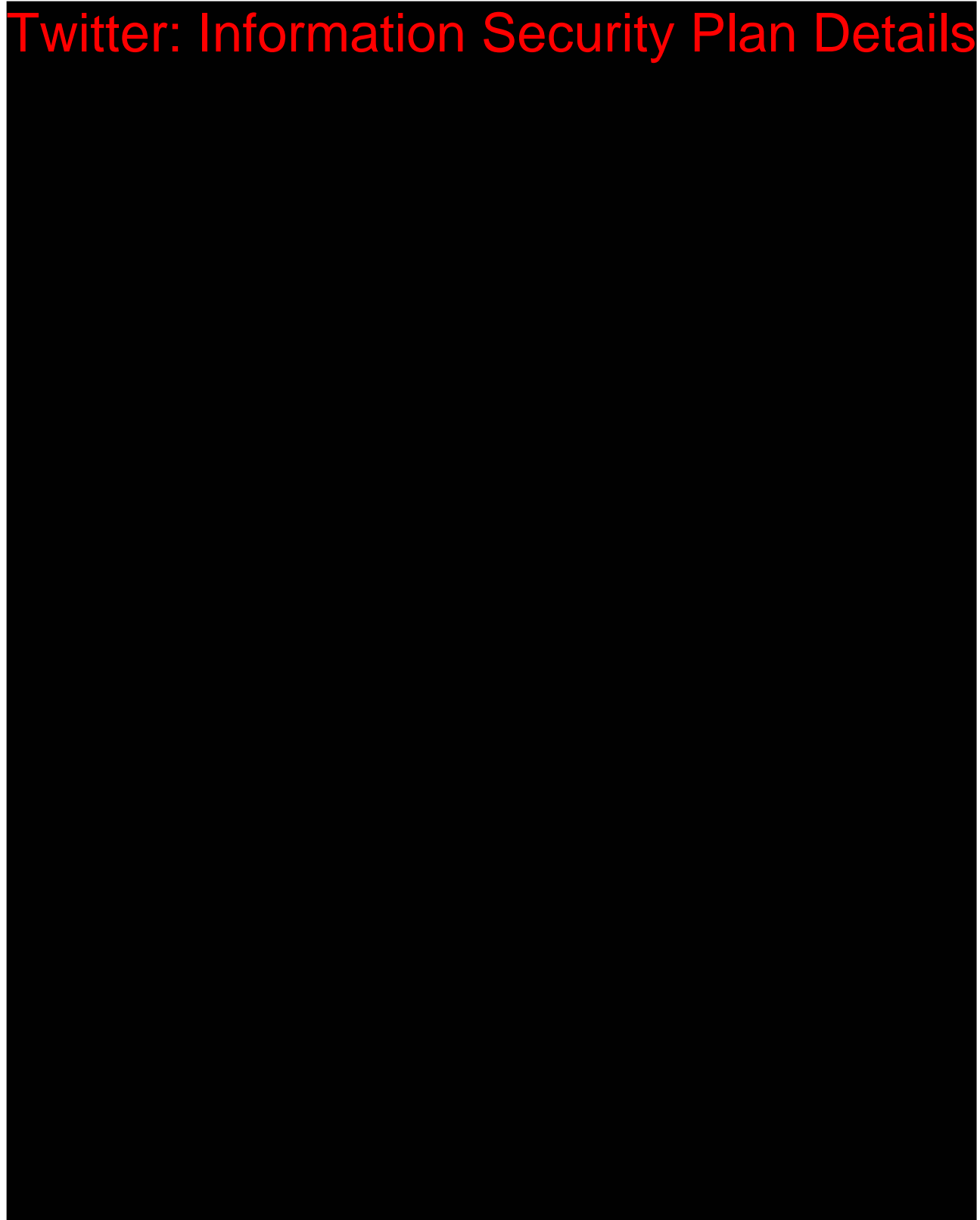
3. Design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

## Twitter: Information Security Plan Details

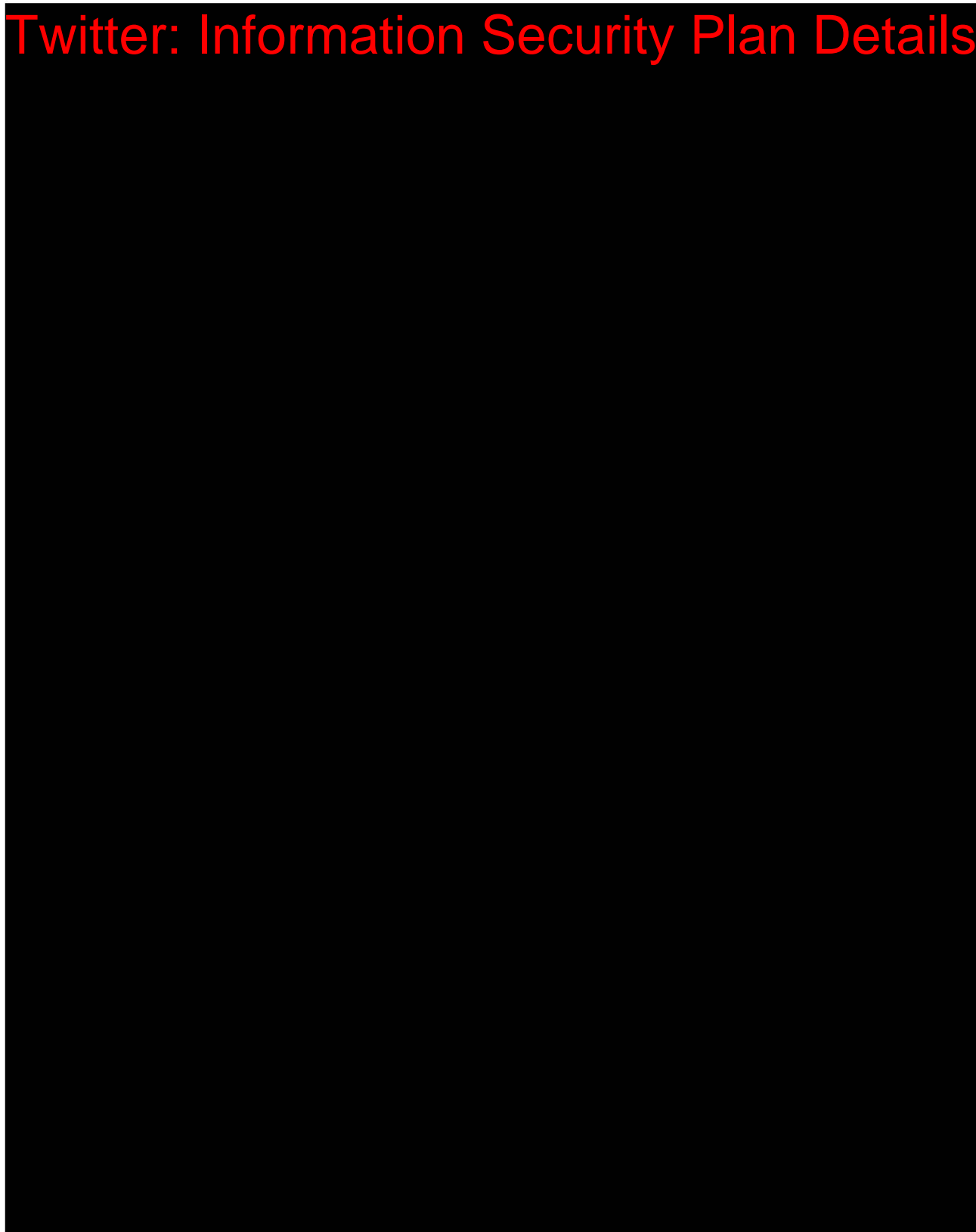
# Twitter: Information Security Plan Details



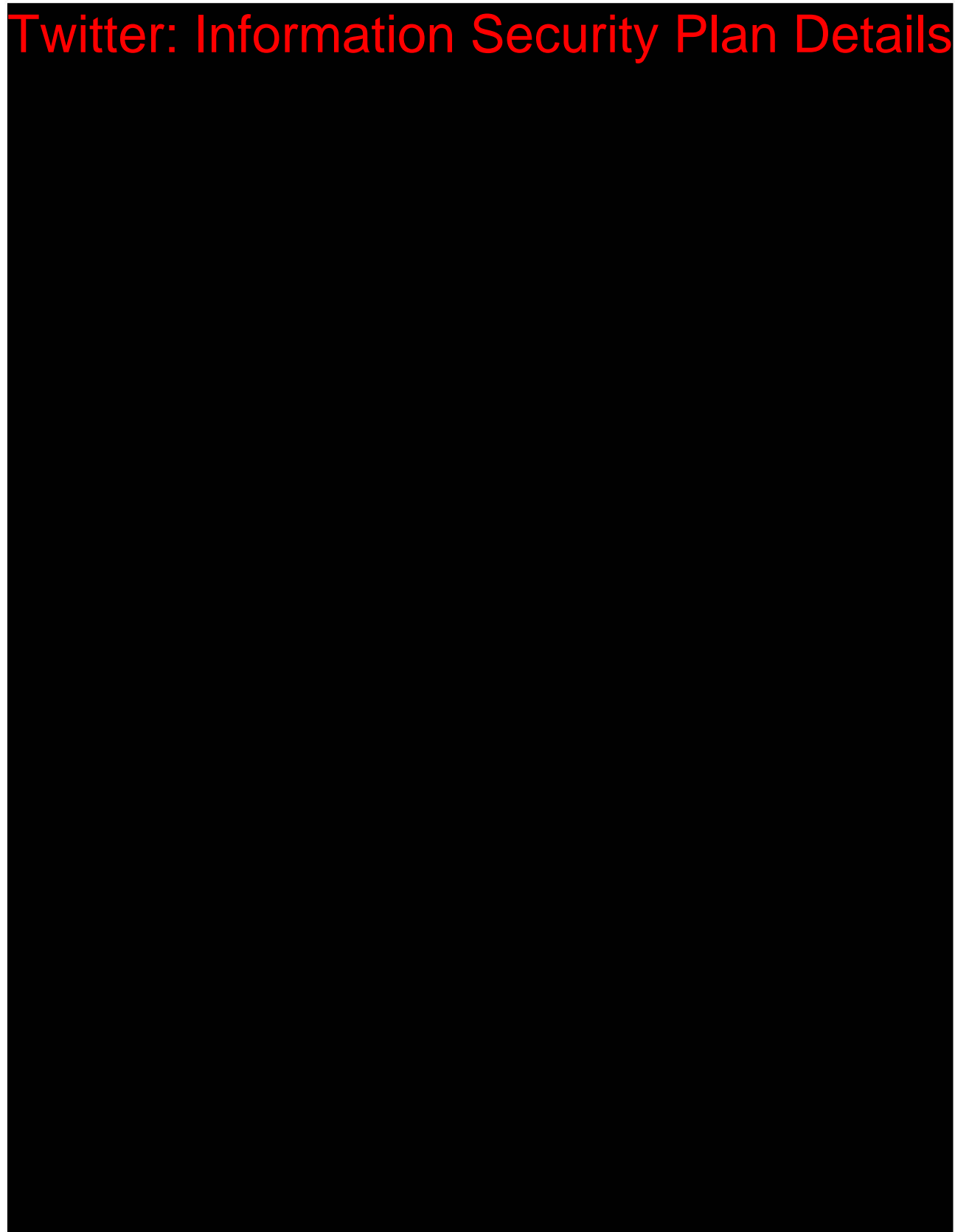
# Twitter: Information Security Plan Details



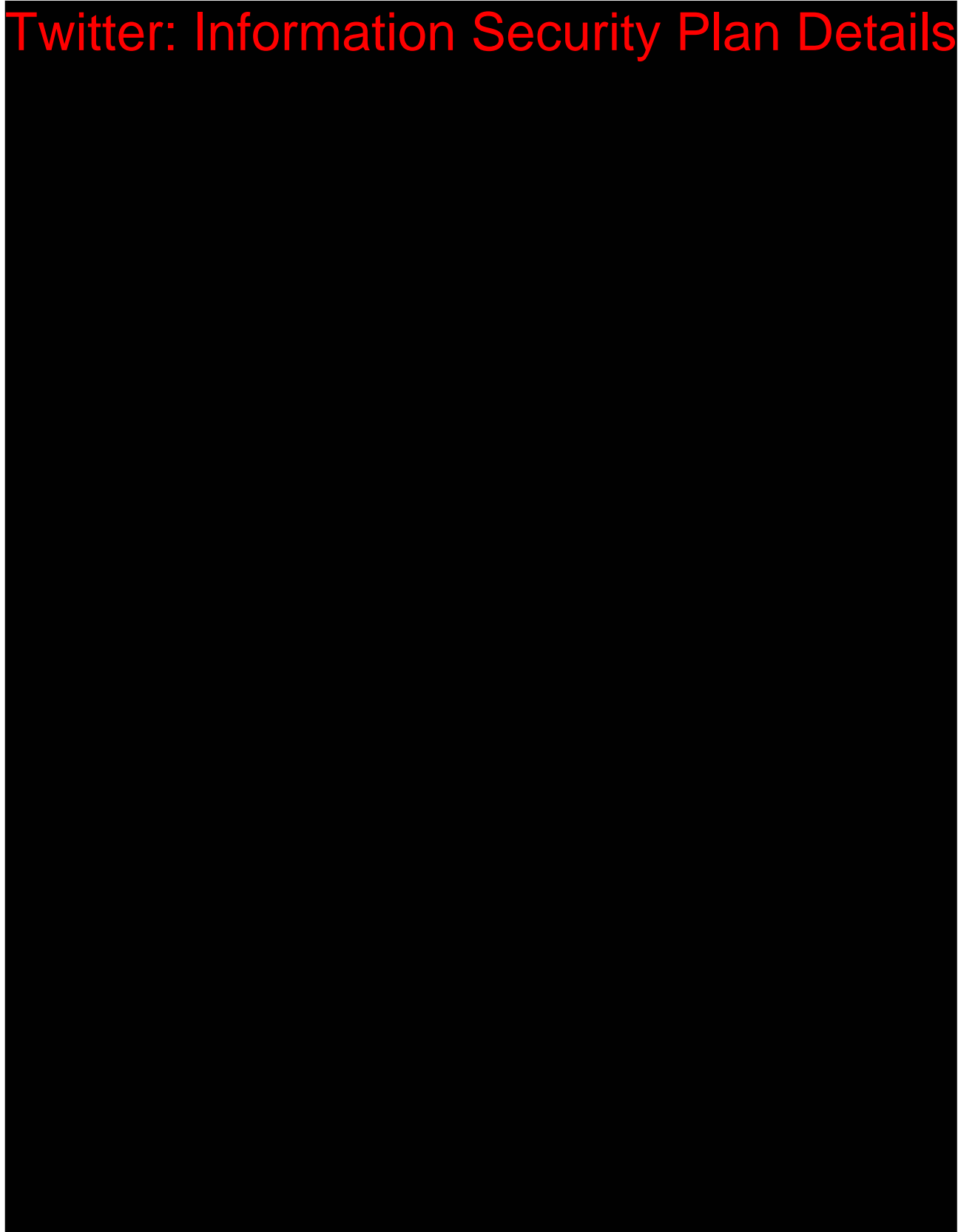
# Twitter: Information Security Plan Details



# Twitter: Information Security Plan Details



# Twitter: Information Security Plan Details





# Twitter: Information Security Plan Details

## Twitter: Information Security Plan Details

4. Development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding nonpublic consumer information such service providers receive from respondent or obtain on Twitter's behalf, and the requirement, by contract, that such service providers implement and maintain appropriate safeguards; provided, however, that this subparagraph shall not apply to personal information about a consumer that respondent provides to a government agency or lawful information supplier when the agency or supplier already possesses the information and uses it only to retrieve, and supply to respondent, additional personal information about the consumer.

Twitter implemented the following controls in order to meet this requirement:

## Twitter: Information Security Plan Details

## Twitter: Information Security Plan Details

5. Evaluation and adjustment of Twitter's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to Twitter's operations or business arrangements, or any other circumstances that Twitter knows or has reason to know may have a material impact on the effectiveness of its information security program.

## Twitter: Information Security Plan Details

# Twitter: Information Security Plan Details

**D. Certify that Twitter's security program is operating with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information and that the program has so operated throughout the reporting period**

As described in the EY Assessment section above, EY performed its assessment of Twitter's Information Security Program in accordance with AICPA Attestation Standards. Refer to the Report for EY's opinion, which provides the conclusion of our assessment.

## Addendum to Transmittal Letter

### Company Overview

Twitter is a real-time information network that connects users to the latest information about what they find interesting. Twitter users search for the public streams they find most compelling and “follow” the conversations. At the heart of Twitter are small bursts of information called “Tweets,” each Tweet being 280 characters in length or less. Twitter users can also follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of approximately half of a billion Tweets per day. As of June 2021, there are 206 million monetizable daily active users on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter has its primary data center in Sacramento, California and a secondary data center in Atlanta, GA.

Twitter, as a company, had only 29 employees in January 2009. At the beginning of 2011, it had approximately 350 employees, and, in September 2013, it had approximately 2,300 employees. As of September 2015, Twitter had approximately 4,200 employees. As of September 2017, Twitter had approximately 3,500 employees. As of September 2019, Twitter had approximately 4,500 employees. As of December 2020, Twitter had approximately 5,500 employees.

Twitter users provide limited profile information, most of which is displayed publicly to all users. When a user creates a Twitter account, the user provides a name, a username, a password, and either an email address, mobile phone number or both. The user may optionally provide a short biography, a location, or a picture. Most of the above information, including the name, username, biography, location, and picture, is listed publicly on the Twitter service.

With regard to the messages sent and received by a user, the majority of these, again, are public. When a user sends a Tweet, it is shared with followers and the rest of the world instantly. Although the default is to make the information public, Twitter does provide settings that allow the Tweets to be “protected,” meaning that the Tweets are shared only with the user’s approved followers. Also, Twitter provides the capability to send a “Direct Message” or “DM” which is a personal message sent via Twitter to other Twitter users. The Direct Message is not viewable by users who are not the Direct Message recipient(s).

## Twitter: Information Security Plan Details

## EY's Assessment of Twitter's Security Program

### Information Security Program Assessment

Over the course of the examination, through discussions with key stakeholders and inspection of documentation, EY reviewed the following aspects of Twitter's Information Security Program:

#### Twitter Information Security Program Governance

The mission of the Information Security organization is to secure Twitter's products and sensitive data. The Security team accomplishes this through a variety of service channels including Security, Governance, Risk & Compliance (SGRC), Security Technology Engineering, Product Security & Architecture, Threat Management & Operations, Adversary Team, and Information Security Strategy & Operations. The Information Security team is led by Chief Information Security Officer (CISO) Rinki Sethi, who was hired in 2020. The CISO reports to Peiter "Mudge" Zetko, Member of Staff and Head of the Confidence organization which includes Information Security, Twitter Service, Enterprise IT, and Privacy Engineering. Mudge reports to Jack Dorsey, Chief Executive Officer.

Information Security objectives are included in our company-wide planning process and include major initiatives (new) and run the business security activities. InfoSec specific progress on our objectives are tracked by the CISO and reported to Senior Management at periodic intervals. On an annual basis, InfoSec produces a holistic Information Security Risk Assessment and shares results with relevant internal oversight groups including but not limited to Legal, Compliance, Internal Audit, etc. On a regular basis, the CISO hosts sessions to discuss security trends, top risks / their treatment, rising risks, and a look back at recent security incidents.

## Twitter: Information Security Plan Details

# Twitter: Information Security Plan Details

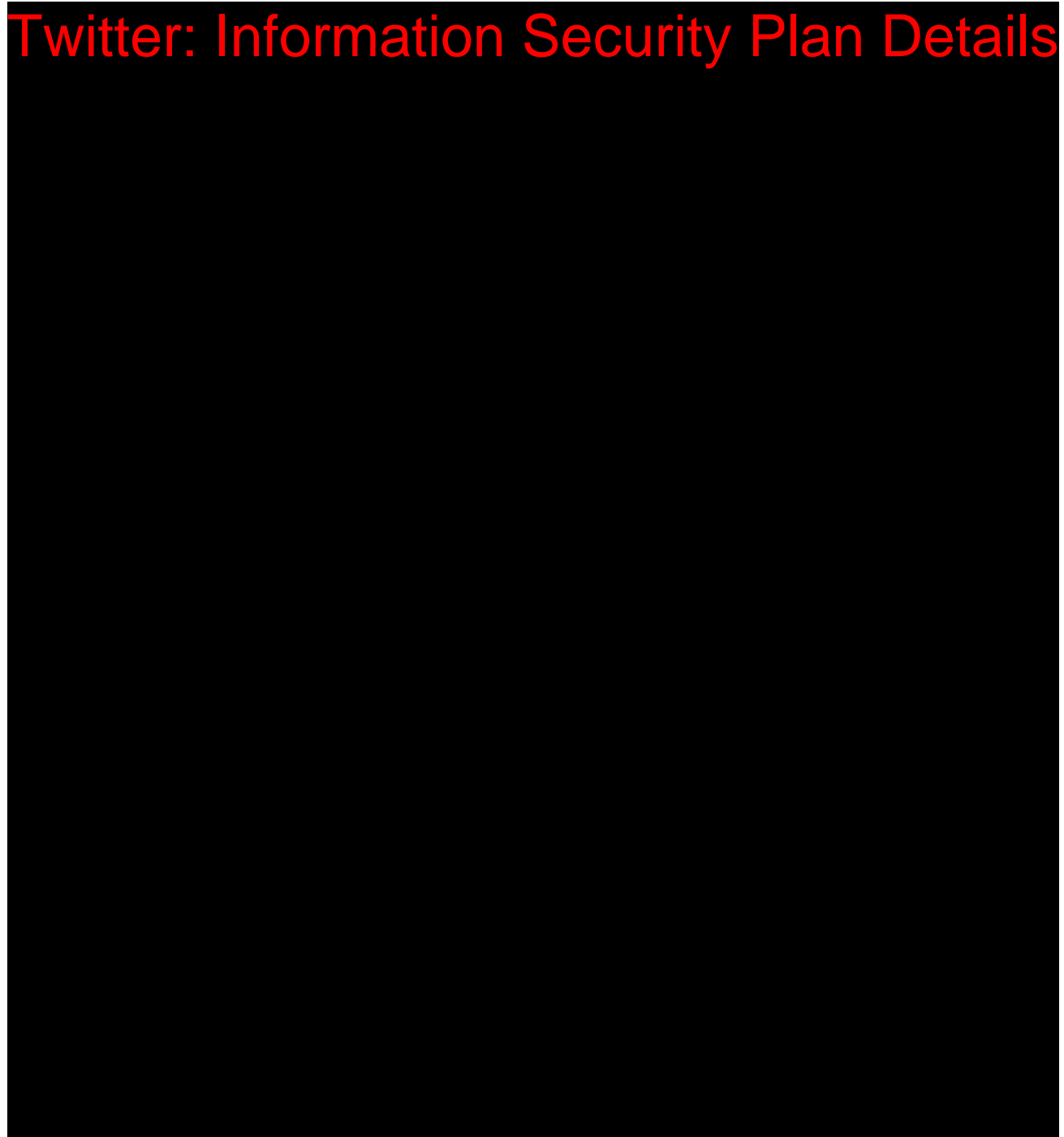
## Twitter Information Security Program Scope

Twitter has one primary product/service offering, namely the Twitter service. Accordingly, the relevant business/product scoping is the Twitter service for purposes of the Order. To further define the scope of Twitter's Information Security Program for purposes of the Order, Twitter continuously performs a risk assessment, as described below, using the ISO/IEC 27002:2013 framework. As part of its ongoing risk assessment process, Twitter considers the size, complexity, nature and scope of activities, and amount and nature of non-public consumer information it collects from or about consumers and adjusts its security program, considering changes to its business. Additional details regarding Twitter's risk assessment process are described in the section below.

## Risk Assessment Process

# Twitter: Information Security Plan Details

# Twitter: Information Security Plan Details



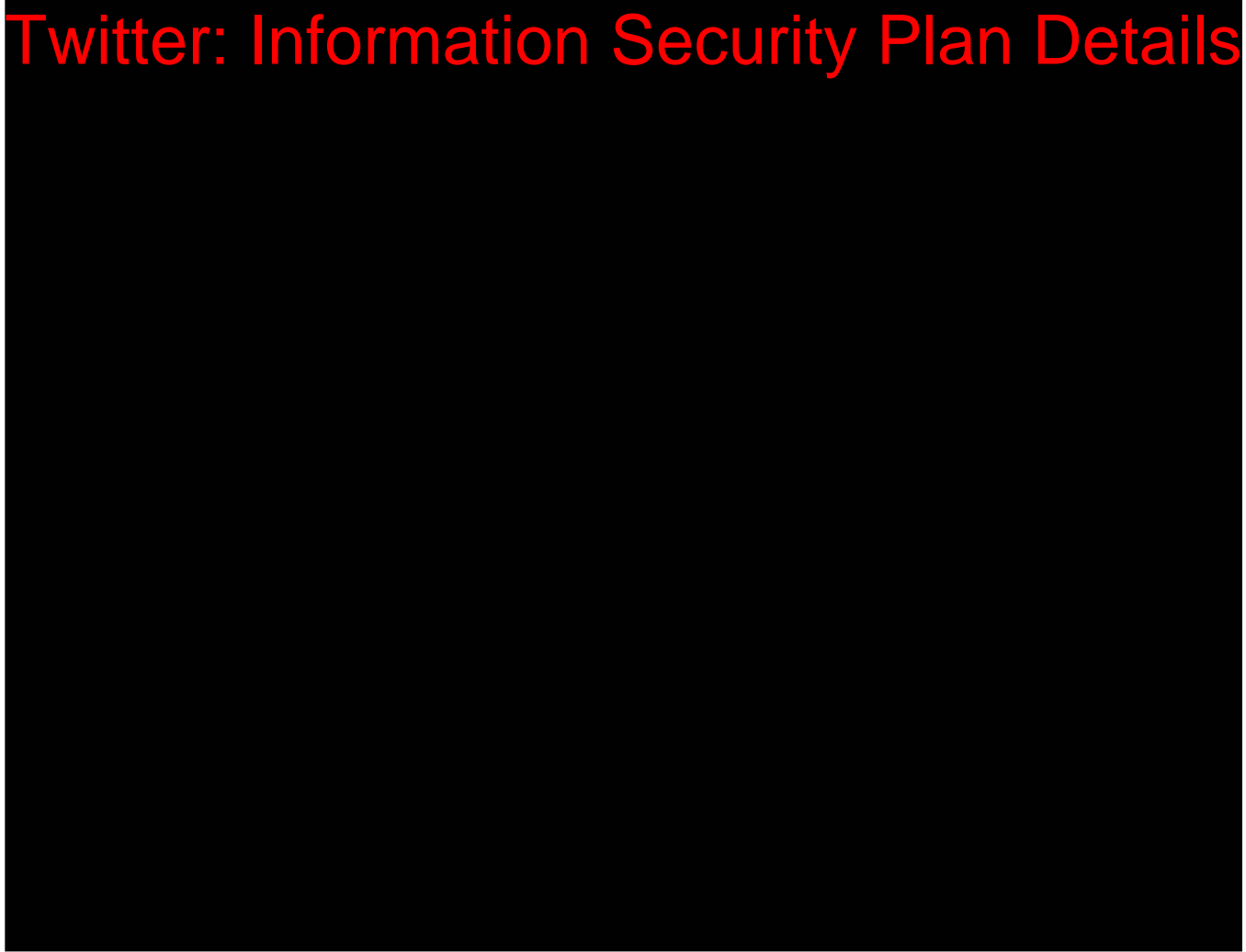
## Data Classification

As part of the ongoing Twitter risk assessment process, the following data types on Twitter information systems are determined as being within the scope of the Order.

# Twitter: Information Security Plan Details



# Twitter: Information Security Plan Details



## Report of Independent Accountants

To the Management of Twitter:

We have examined Management's Assertion ("Assertion" included in Exhibit I) that as of, and for the two years ended, September 12, 2021 (the "Reporting Period"), in accordance with Parts II and III of the Decision and Order ("the Order") issued by the U.S. Federal Trade Commission ("FTC") on March 2, 2011:

- The Company established and implemented a comprehensive information security program ("Twitter Information Security Program" or "Subject Matter") based on the Internal Organization for Standardization ("ISO") / International Electrotechnical Commission ("IEC") Standard 27002:2013 ("ISO/IEC 27002:2013")
- The Company conducted a risk assessment to identify material risks, both internal and external, and assessed the sufficiency of the safeguards in place to control those risks which could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of non-public consumer information or in unauthorized administrative control of the Twitter system
- The Company's administrative, technical, and physical safeguards within the Twitter Information Security Program are appropriate to its size and complexity, the nature and scope of Twitter's activities, and the sensitivity of non-public consumer information collected from consumers.
- The Company's security controls meet or exceed the protections required by Part II of the Order
- The Twitter Information Security Program operated with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of non-public consumer information (as defined by the Order), and the program has so operated throughout the reporting period

The Company's management is responsible for its Assertion. Our responsibility is to express an opinion on the Assertion based on an examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Those standards require that an examination is planned and performed to obtain reasonable assurance about whether the Assertion is fairly stated in all material respects. An examination involves performing procedures to obtain evidence about the Assertion. The nature, timing, and extent of the procedures selected dependent on our judgment, including an assessment of the risks of material misstatement of the Assertion, whether due to fraud or error. The evidence obtained is sufficient and appropriate to provide a reasonable basis for the opinion.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to meet the applicable criteria. Also, the

projection to the future of conclusions about the operating effectiveness of the controls to meet the applicable criteria is subject to the risk that the system may change or that controls may become ineffective.

We are not responsible for Twitter's interpretation of, or compliance with, security-related laws, statutes, and regulations applicable to Twitter in the jurisdictions within which Twitter operates.

We are also not responsible for Twitter's interpretation of, or compliance with, security-related self-regulatory frameworks. Accordingly, no opinion or other form of assurance on Twitter's interpretation of, or compliance with, the security-related laws, statutes, regulations, or security-related self-regulatory frameworks with which Twitter has committed to comply is expressed in this report.

The report concludes that the Assertion fairly states that for the period September 13, 2019 to September 12, 2021:

- The Company established and implemented a comprehensive information security program ("Twitter Information Security Program" or "Subject Matter") based on the Internal Organization for Standardization ("ISO") / International Electrotechnical Commission ("IEC") Standard 27002:2013 ("ISO/IEC 27002:2013")
- The Company conducted a risk assessment to identify material risks, both internal and external, and assessed the sufficiency of the safeguards in place to control those risks which could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of non-public consumer information or in unauthorized administrative control of the Twitter system
- The Company's administrative, technical, and physical safeguards within the Twitter Information Security Program are appropriate to its size and complexity, the nature and scope of Twitter's activities, and the sensitivity of non-public consumer information collected from consumers.
- The Company's security controls meet or exceed the protections required by Part II of the Order.
- The Twitter Information Security Program operated with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of non-public consumer information (as defined by the Order), and the program has so operated throughout the reporting period

This report is intended solely for the information and use of the management of Twitter and the FTC in connection with the Order and is not intended to be and should not be used by anyone other than these specified parties.

*Ernst & Young LLP*

11 November 2021



1355 Market Street  
San Francisco  
California  
94103

twitter.com

## Exhibit I

### Twitter's Management's Assertion

The management of Twitter (or the "Company") asserts that as of and for the two years ended September 12, 2021 (the "Reporting Period"), in accordance with Parts II and III of the Decision and Order (the "Order"), issued date March 2, 2011, between Twitter and the U.S. Federal Trade Commission ("FTC"):


- The Company established and implemented a comprehensive information security program ("Twitter Information Security Program" or "Subject Matter") based on the International Organization for Standardization ("ISO") / International Electrotechnical Commission ("IEC") Standard 27002:2013 ("ISO/IEC 27002:2013")
- The Company conducted a risk assessment to identify material risk, both internal and external, and assessed the sufficiency of the safeguards in place to control those risks which could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of nonpublic consumer information or in unauthorized administrative control of the Twitter system
- The Company's administrative, technical, and physical safeguards within the Twitter Information Security Program are appropriate to its size and complexity, the nature and scope of Twitter's activities, and the sensitivity of nonpublic personal information collected from consumers.
- The Company's security controls meet or exceed the protections required by Parts II of the Order
- The Twitter Information Security Program operated with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information (as defined by the Order), and the program has so operated throughout the reporting period

Twitter's Information Security Controls are in scope for the FTC issued Consent Decree, for the reporting period 13 September 2019 to 12 September 2021. Twitter designed these controls to provide reasonable assurance that the criteria set forth in the consent decree were achieved based on the ISO 27002:2013 control framework.

We are responsible for designing, implementing, operating, and monitoring effective controls over the information security program. We are also responsible for identifying the standard on which our program is based and the risks that would threaten the achievement of such criteria.

We assessed whether the controls were implemented and operated for the period 13 September 2019 to 12 September 2021 based on the Criteria. Based on that assessment, we assert that we have maintained, in all material respects, effective controls over Information Security for the period 13 September 2019 to 12 September 2021 based on the criteria set forth by the FTC Consent Decree.

Twitter, Inc.

By:   
Sean Edgett  
General Counsel

By:   
Damien Kieran (Nov 11, 2021 11:31 PST)  
Chief Privacy Officer

**Attachment A:**

**Twitter's Information Security Program Criteria, Supporting Controls, Test Procedures, and Assessment Results**

The table below sets forth the Twitter Information Security Program Criteria, supporting controls, and Assessment results. This attachment must be read in conjunction with the Report of Independent Accountants provided on pages 24-25.

Twitter: Information Security Plan Details			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
Twitter: Information Security Plan Details			No deviation noted.
			No deviation noted.
Twitter: Information Security Plan Details			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
Twitter: Information Security Plan Details			No deviation noted.
			No deviation noted.

<b>Twitter: Information Security Plan Details</b>			Not Applicable
			No deviation noted.
			Not Applicable
			No deviation noted.
			Not Applicable
<b>Twitter: Information Security Plan Details</b>			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<b>Twitter: Information Security Plan Details</b>			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

# Twitter: Information Security Plan Details

# Twitter: Information Security Plan Details

Not Applicable



# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

# Twitter: Information Security Plan Details



# Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
Twitter: Information Security Plan Details			No deviation noted.

# Twitter: Information Security Plan Details

## Twitter: Information Security Plan Details

No deviation noted.

# Twitter: Information Security Plan Details

Not Applicable

No deviation noted.

No deviation noted.

No deviation noted.

## Twitter: Information Security Plan Details

No deviation noted.

Not Applicable

No deviation noted.

No deviation noted.

No deviation noted.

<b>Twitter: Information Security Plan Details</b>			Not Applicable
<b>Twitter: Information Security Plan Details</b>			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<b>Twitter: Information Security Plan Details</b>			No deviation noted.
<b>Twitter: Information Security Plan Details</b>			No deviation noted.
<b>Twitter: Information Security Plan Details</b>			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

No deviation noted.



# Twitter: Information Security Plan Details



# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

Not Applicable

Not Applicable

Not Applicable

No deviation noted.

# Twitter: Information Security Plan Details



# Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p>Twitter: Information Security Plan Details</p>			No deviation noted.
			No deviation noted.

## Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<h2>Twitter: Information Security Plan Details</h2>			No deviation noted.
			No deviation noted.
			No deviation noted.
			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

Not Applicable

No deviation noted.

Not Applicable

Not Applicable

Not Applicable

# Twitter: Information Security Plan Details

No deviation noted.

Not Applicable

Not Applicable

No deviation noted.



# Twitter: Information Security Plan Details

No deviation noted.

Not Applicable

No deviation noted.

Twitter: Information Security Plan Details			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
Twitter: Information Security Plan Details			No deviation noted.
			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

## Twitter: Information Security Plan Details

No deviation noted.

The risk associated with this control was addressed by Twitter control 9.4.5. Refer to 9.4.5 attestation.

The risk associated with this control was addressed by Twitter control 9.4.5. Please refer to 9.4.5 attestation.

# Twitter: Information Security Plan Details

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

## Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<b>Twitter: Information Security Plan Details</b>			No deviation noted.
			No deviation noted.



# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

Not Applicable

No deviation noted.

Not Applicable

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

## Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<b>Twitter: Information Security Plan Details</b>			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

Not Applicable

No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

No deviation noted.

# Twitter: Information Security Plan Details

[Redacted]	No deviation noted.
[Redacted]	No deviation noted.
[Redacted]	No deviation noted.
[Redacted]	No deviation noted.

## Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p><b>Twitter: Information Security Plan Details</b></p>			<p>No deviation noted.</p>
			<p>No deviation noted.</p>

Twitter: Information Security Plan Details			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
Twitter: Information Security Plan Details			Not Applicable
Twitter: Information Security Plan Details			Not Applicable
Twitter: Information Security Plan Details			No deviation noted.
Twitter: Information Security Plan Details			No deviation noted.
Twitter: Information Security Plan Details			No deviation noted.
Twitter: Information Security Plan Details			Not Applicable
Twitter: Information Security Plan Details			Not Applicable



# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

**Twitter: Information Security Plan Details**

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<b>Twitter: Information Security Plan Details</b>			No deviation noted.
			No deviation noted.

**Twitter: Information Security Plan Details**

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<b>Twitter: Information Security Plan Details</b>			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

No deviation noted.

# Twitter: Information Security Plan Details

Not Applicable

No deviation noted.

## Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p><b>Twitter: Information Security Plan Details</b></p>			No deviation noted.
			No deviation noted.
			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

## Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<h1>Twitter: Information Security Plan Details</h1>			

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

No deviation noted.



Twitter: Information Security Plan Details			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p><b>Twitter: Information Security Plan Details</b></p>			No deviation noted.
			No deviation noted.

## Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p><b>Twitter: Information Security Plan Details</b></p>			No deviation noted.
			No deviation noted.
			No deviation noted.
			No deviation noted.

## Twitter: Information Security Plan Details

No deviation noted.

# Twitter: Information Security Plan Details



## Twitter: Information Security Plan Details

### Twitter: Information Security Plan Details

No deviation noted.

### Twitter: Information Security Plan Details

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
Twitter: Information Security Plan Details			No deviation noted.
Twitter: Information Security Plan Details			No deviation noted.

**Twitter: Information Security Plan Details**

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p><b>Twitter: Information Security Plan Details</b></p>			No deviation noted.
			No deviation noted.
			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

<b>Twitter: Information Security Plan Details</b>			No deviation noted.
			No deviation noted.
			Not Applicable
<b>Twitter: Information Security Plan Details</b>			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<b>Twitter: Information Security Plan Details</b>			No deviation noted.



# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

Twitter: Information Security Plan Details			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p style="color: red; font-size: 2em; font-weight: bold;">Twitter: Information Security Plan Details</p>			No deviation noted.
			No deviation noted.
			No deviation noted.

Twitter: Information Security Plan Details			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
Twitter: Information Security Plan Details			No deviation noted.
Twitter: Information Security Plan Details			
Control ID	Twitter Control Description	EY's Test Procedures	Result Details
Twitter: Information Security Plan Details			No deviation noted.
Twitter: Information Security Plan Details			No deviation noted.

# Twitter: Information Security Plan Details

No deviation noted.

No deviation noted.

No deviation noted.

**Twitter: Information Security Plan Details**

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p><b>Twitter: Information Security Plan Details</b></p>			<p>No deviation noted.</p>

**Twitter: Information Security Plan Details**

Control ID	Twitter Control Description	EY's Test Procedures	Result Details
<p><b>Twitter: Information Security Plan Details</b></p>			<p>No deviation noted.</p>

Attachment B:

Assessment Interviews Summary

Role	Team
<b>Twitter: Confidential/Trade Secret Information</b>	

Role	Team
<b>Twitter: Confidential/Trade Secret Information</b>	

Role	Team
<b>Twitter: Confidential/Trade Secret Information</b>	