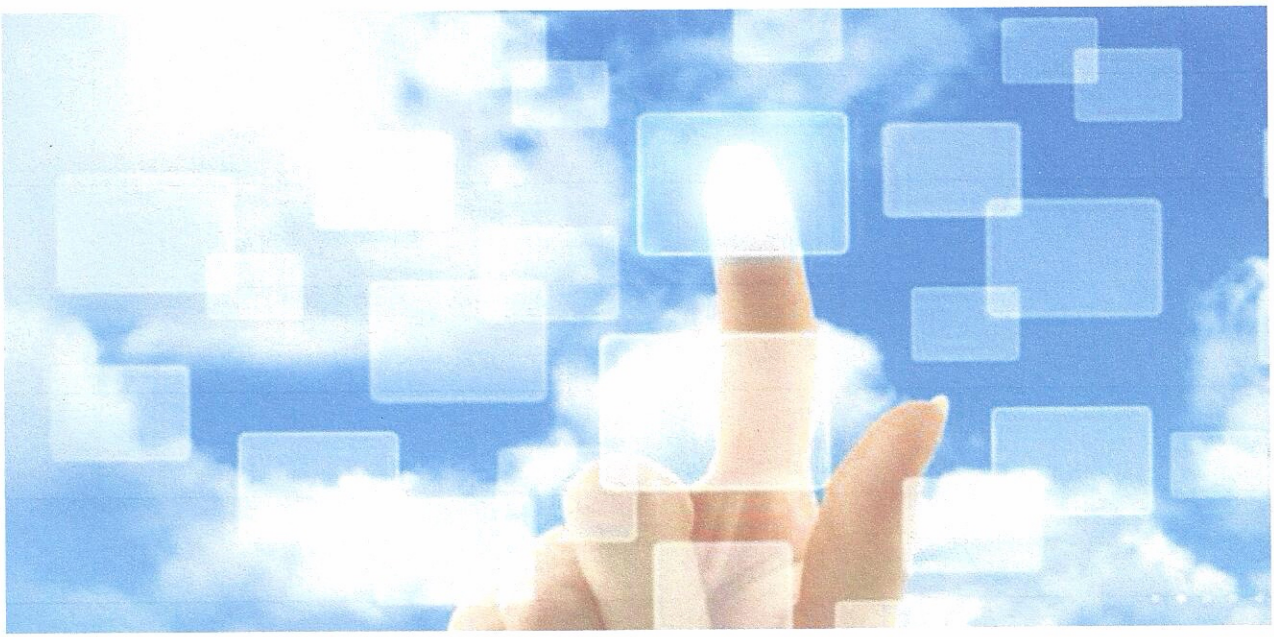
Highstreet

Report on Highstreet IT Solutions, LLC's Description of Network, Application and Cloud Services System, and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Availability, Processing Integrity, and Confidentiality

For the Period October 1, 2024, to September 30, 2025



Highstreet

TABLE OF CONTENTS

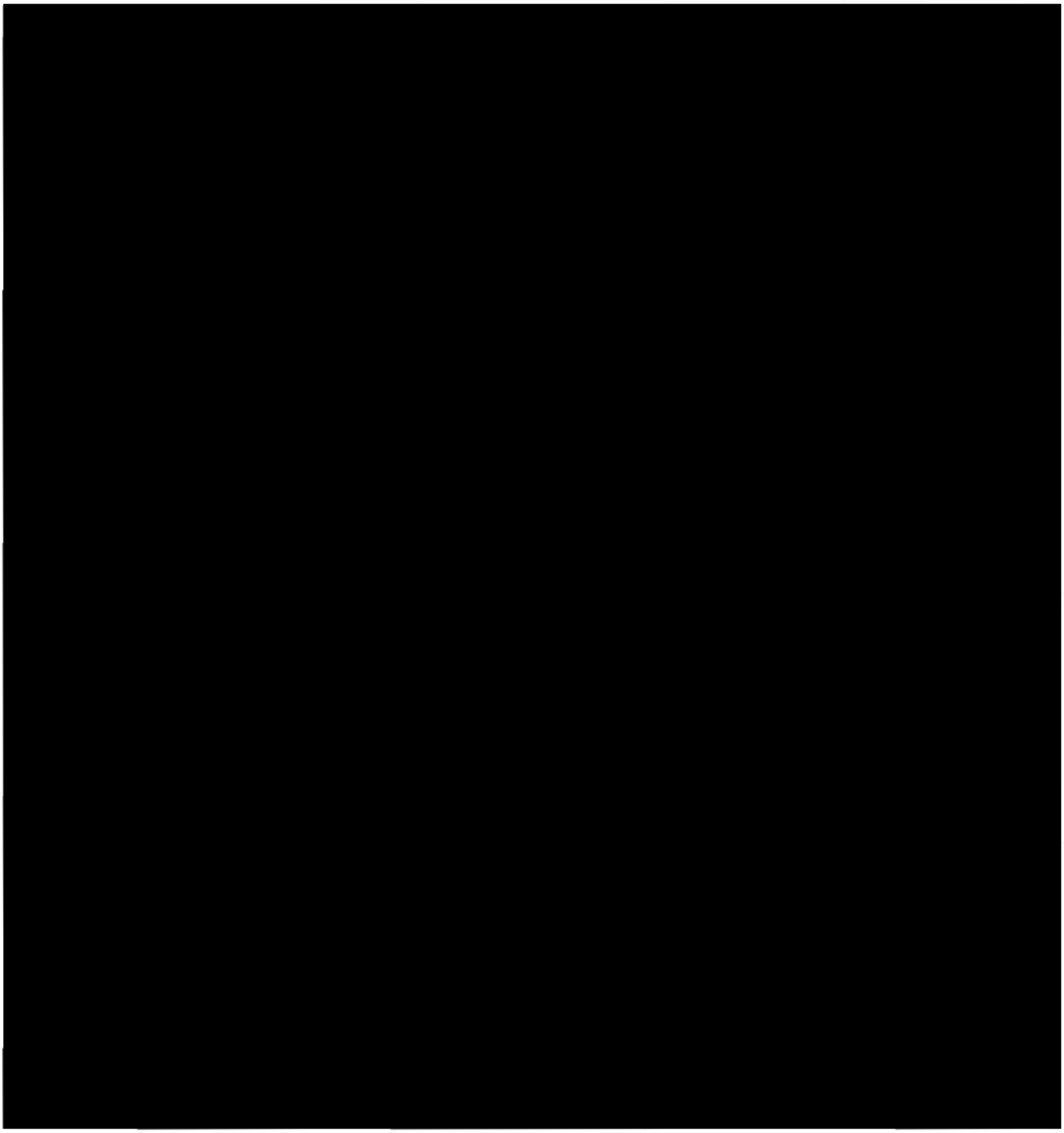
SECTION I - INDEPENDENT SERVICE AUDITORS' REPORT I
SECTION II - HIGHSTREET SERVICES SYSTEM MANAGEMENT ASSERTION 1
SECTION III - DESCRIPTION OF HIGHSTREET'S NETWORK AND APPLICATION SOLUTIONS AND CLOUD SERVICES SYSTEM 3
COMPANY OVERVIEW 3
LEADERSHIP 3
HIGHSTREET ORGANIZATION CHART 4
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 6
PRINCIPAL SYSTEM REQUIREMENTS 6
COMPONENTS OF THE SYSTEM USED TO PROVIDE SERVICE 6
OTHER ASPECTS OF THE INTERNAL CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING OF CONTROLS THAT ARE RELEVANT TO THE SERVICES PROVIDED AND THE APPLICABLE TRUST SERVICES CRITERIA 9
MANAGEMENT PHILOSOPHY 9
CONTROL ENVIRONMENT 9
CODE OF ETHICS 9
ORGANIZATIONAL STRUCTURE AND ASSIGNMENT OF AUTHORITY & RESPONSIBILITY 9
COMMITMENT TO COMPETENCE 10
COMMUNICATION AND ENFORCEMENT OF INTEGRITY AND ETHICAL VALUES 10
CONTROL ACTIVITIES-SECURITY 11
CONTROL ACTIVITIES - AVAILABILITY AND PROCESSING INTEGRITY 14
CONTROL ACTIVITIES - CONFIDENTIALITY 14
INFORMATION & COMMUNICATION 15
COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS 16
COMPLEMENTARY USER ENTITY CONTROL CONSIDERATIONS 17
SECTION IV - HIGHSTREET'S SECURITY, AVAILABILITY, PROCESSING INTEGRITY, AND CONFIDENTIALITY TRUST SERVICES AND RELATED CONTROLS AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS OF TESTS 21
INTRODUCTION 21
TESTS OF OPERATING EFFECTIVENESS 21
TYPES AND DESCRIPTIONS OF THE TESTS OF OPERATING EFFECTIVENESS 22
SAMPLING 22
TEST RESULTS 22

eDelta CPA Services

eDelta CPA Services, P.C.
370 Lexington Avenue, Suite 1002
New York, New York 10017

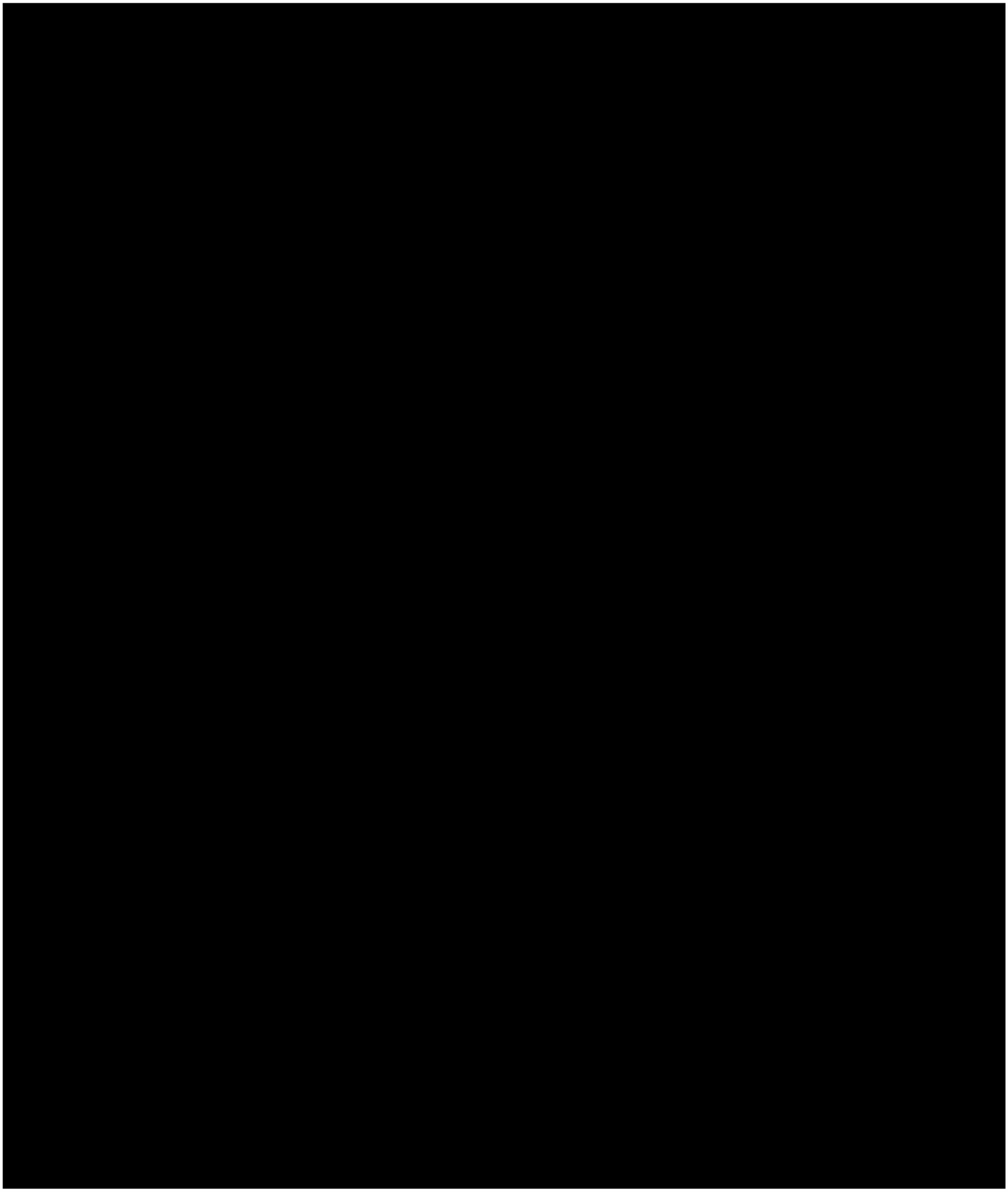
Phone: 646-205-9960
Fax: 631-389-2395

Section I - Independent Service Auditors' Report



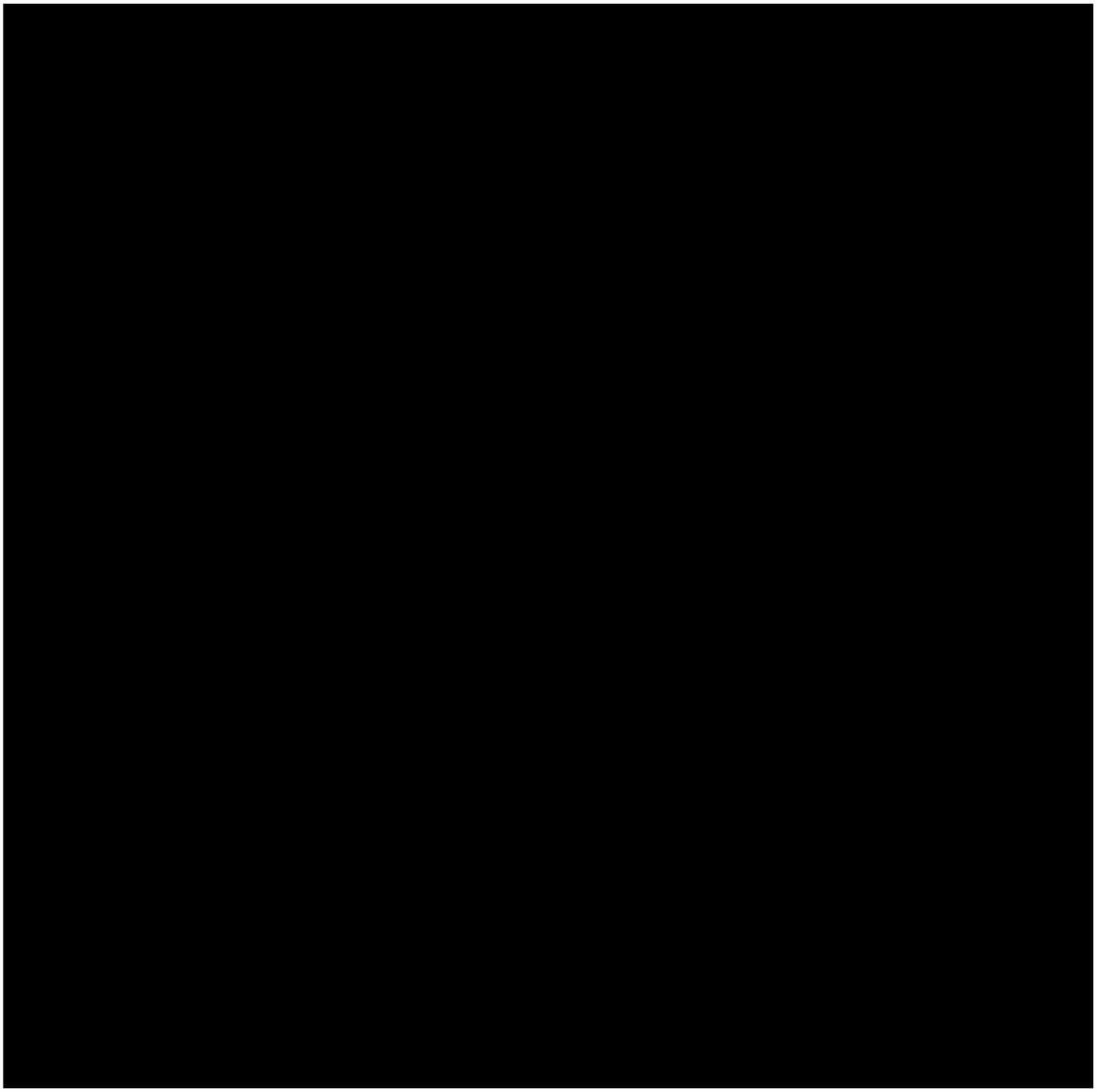
eDelta CPA Services, P.C.
370 Lexington Avenue, Suite 1002
New York, New York 10017

Phone: 646-205-9960
Fax: 631-389-2395



eDelta CPA Services, P.C.
370 Lexington Avenue, Suite 1002
New York, New York 10017

Phone: 646-205-9960
Fax: 631-389-2395



Opinion

In our opinion, in all material respects,

a. The description presents Highstreet's Services in-scope System that was designed and implemented throughout the period October 1, 2024, to September 30, 2025, in accordance with the description criteria.

eDelta CPA Services, P.C.
370 Lexington Avenue, Suite 1002
New York, New York 10017

Phone: 646-205-9960
Fax: 631-389-2395

b. The controls stated in the description were suitably designed throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that (a) Highstreet Services System service commitments and systems requirements would be achieved based on the applicable Trust Services Criteria would be achieved; (b) the control activity set forth would be achieved; and (c) the control objectives set forth would be achieved, if the controls operated effectively throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that (a) Highstreet Services System service commitments and system requirements were achieved based on the applicable Trust Services Criteria; (b) the control activity specified were achieved; and (c) the control objectives set forth were achieved.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Highstreet Services System, user entities of the in-scope for Highstreet Services System during some or all of the period October 1, 2024 to September 30, 2025, business partners of Highstreet Services System subject to risks arising from interactions with Highstreet Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization.
- How the Service Organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the Service Organization's services.
- The applicable Trust Services Criteria, the control activity specified, and the control objectives set forth.
- The risks that may threaten the achievement of the Service Organization's service commitments and system requirements and how controls address those risks.

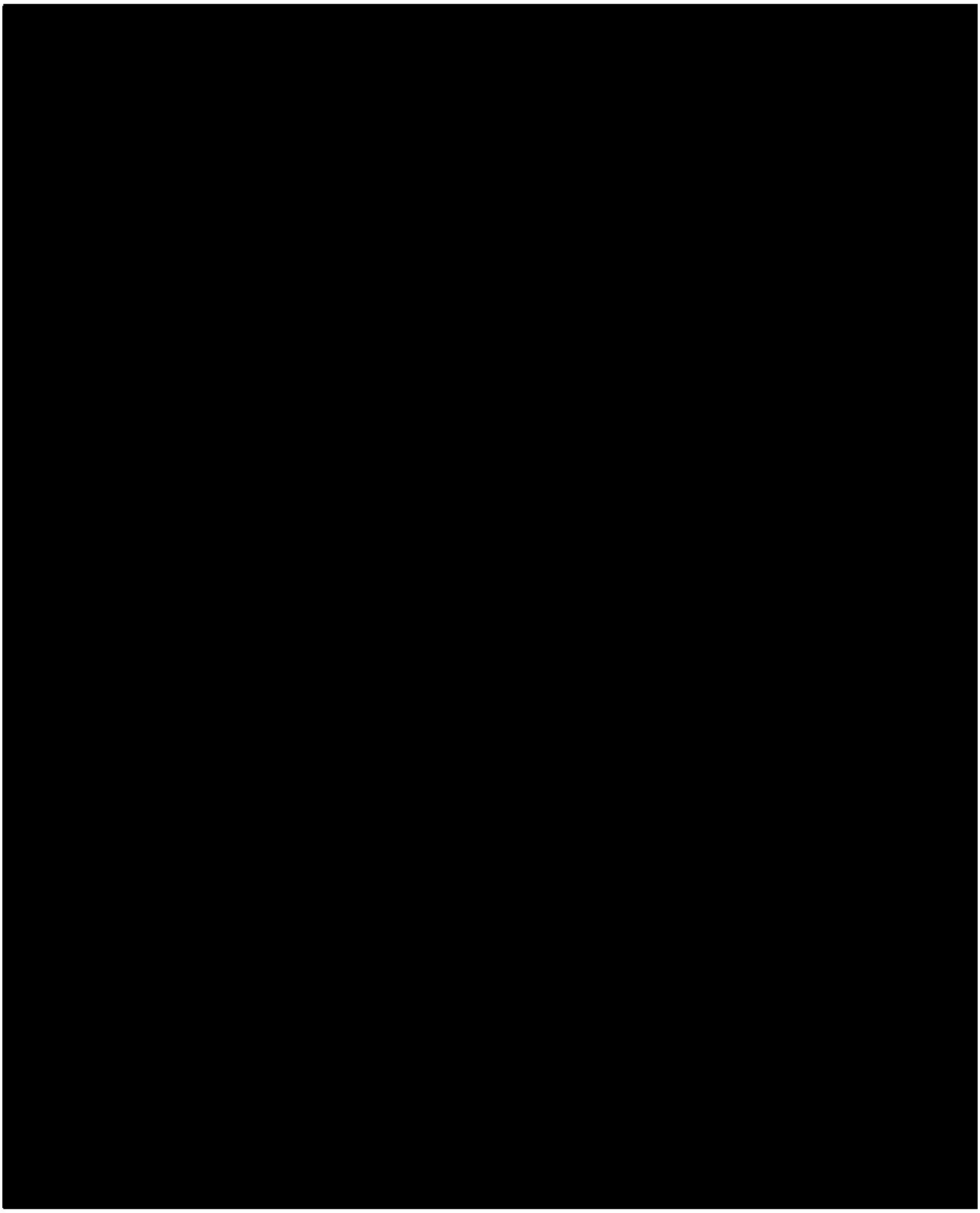
This report is not intended to be, and should not be, used by anyone other than these specified parties.

eDelta CPA Services, P.C.

New York, NY.

November 11, 2025

Highstreet



Highstreet



Highstreet

Section III - Description of Highstreet's Network and Application Solutions and Cloud Services System

Company Overview

Highstreet IT Solutions, LLC ("Highstreet" or the "Company") provides ERP, application, and Hosting services to clients. Highstreet's custom-built services deliver ERP solutions, through a public cloud using AWS and the Oracle Cloud Infrastructure (OCI).

Leadership

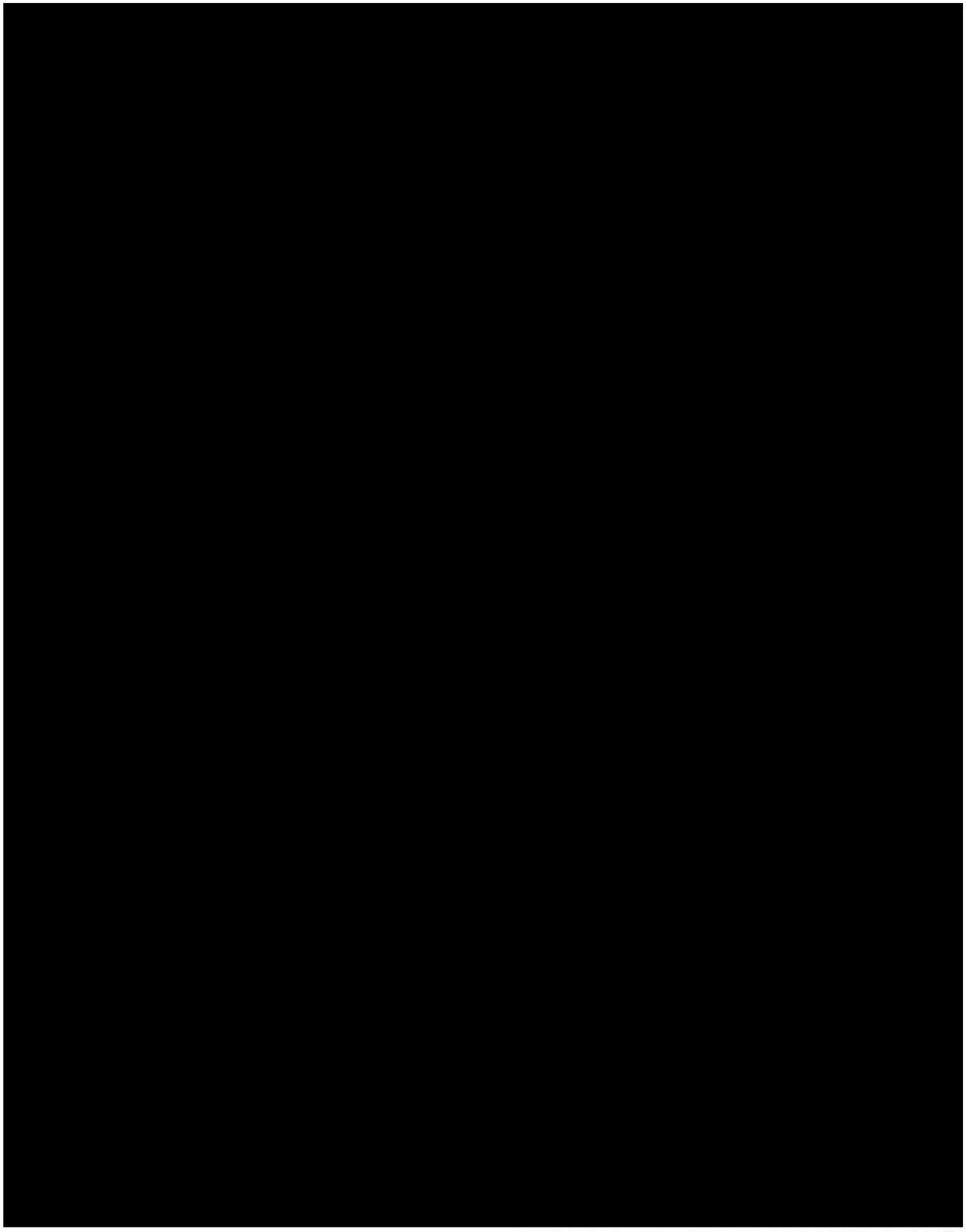
The Company has organized leadership and defined policies related to information security to ensure alignment with business objectives to adequately serve clients. Roles and responsibilities for teams and team members within the organization are defined within the Company's organizational structure and reporting lines (see organization chart) as well as written job descriptions.

Management reviews the Company's organizational structure at least annually as part of strategic planning and any changes are made as needed based on changing reporting lines, authorities, and responsibilities.

Management also communicates expected behavior and responsibilities via the Employee Handbook and the Contractor Handbook. Workforce members are provided with one of the two handbooks as part of onboarding, depending on the nature of their business relationship with the Company.

Highstreet

Highstreet Organization Chart



Highstreet

Highstreet Organization Chart (Continued)



[redacted]

Principal System Requirements

Highstreet establishes operational and system requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Highstreet's system policies and procedures, system design documentation, and in contracts with customers. Highstreet principal system requirements include the following:

Components of the System Used to Provide Service

Infrastructure

IT infrastructure components utilized to support Highstreet customers, include, but may not be limited to the following:

Infrastructure System	Description
[redacted]	

Primary Software

Highstreet software/application tools used to support customer services, include:

Applications/Tools	Description
Remote Access	
[redacted]	
Network and Server Management	
[redacted]	

Highstreet

Network and Server Monitoring	[redacted]
Network Security	[redacted]

People

Highstreet's organizational structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job responsibilities. The structure provides defined responsibilities and lines of authority for reporting and communication. The assignment of roles and responsibilities within the various departments provides effective segregation of duties.

Background checks are performed on all Highstreet employees, contractors and third parties in accordance with their roles and responsibilities, job function, and level of access to sensitive or classified information. Every employee, as well as contractors and third parties, are required to sign a Confidentiality/Non-Disclosure Agreement as a condition of employment and/or statement of work. Confidentiality/Non-Disclosure Agreements are stored in the employee's personnel file or within the Legal Department.

Highstreet's Customer Services are provided by its' internal Information Technology and Security Department (ITS), and through its' Sub-Service Provider [redacted]

The ITS Department provides the following services:

- Information Technology Policies, Procedures and Standards.
- Network and Server Management, and Administration (including Performance and Capacity).
- Infrastructure Upgrades and Software Updates (including Patch Management).
- Business Continuity and Disaster Recovery.

With regards to Information Security, the Highstreet ITS Department is responsible for:

- Reviewing, assessing, and enforcing the Highstreet Security Policy
- Physical security and logical network access management, including:
  - New user setup.
  - Modifications to existing user access.
  - Removal of terminated user access.
- Management and support of firewalls, servers, and other networked devices. Highstreet also offers and performs network support including, but not limited to:
  - File and directory services, maintenance, and usage/security monitoring.
- Establishing and monitoring internet and network connectivity both internally and externally.
- Providing capacity management for the environment that is agreed to in the contract.
- The protection of core servers and services against the threat of virus and spyware attacks.
- Performance of the infrastructure change management processes, including patch management.
- Providing Helpdesk Levels 1, 2, and 3 support for internal hardware, including servers, desktops and laptops, printers, and other peripherals.

- Assessing and reporting incident trends with recommendations for improvement.
- Providing primary support and coordination for Business Continuity and Disaster Recovery planning.

Key Highstreet Customer Services personnel include, but are not limited to, the following:

Global Management Teams

Highstreet's Global Management Teams in the U.S., Canada, and India, which provide implementation and support services for Company and customer environments.

IT Operations Center (ITOC/NOC) Engineering

Highstreet uses [redacted]T Operations Center (ITOC/NOC) Engineering to provide day-to-day 1st and 2nd level support surrounding infrastructure and desktop technologies. The ITOC/NOC is responsible for all day-to-day hands on operations, including: Incident Management and Request Management as defined by ITIL; troubleshooting network and server problems; troubleshooting desktop device problems; trouble ticket generation and ownership; escalation of Tier 1-2 incidents to resolution; systems monitoring and analysis; responsibility for low-high priority calls at all severity levels; problem Management (determining permanent solutions to unique or chronic problems); documenting resolutions and contributing to internal knowledge-base; maintenance of configuration information and run-books; participation in the Change Management process; and, other requests made by Company management. Highstreet has documented policies and procedures to support the operations and controls over its Services.

Data

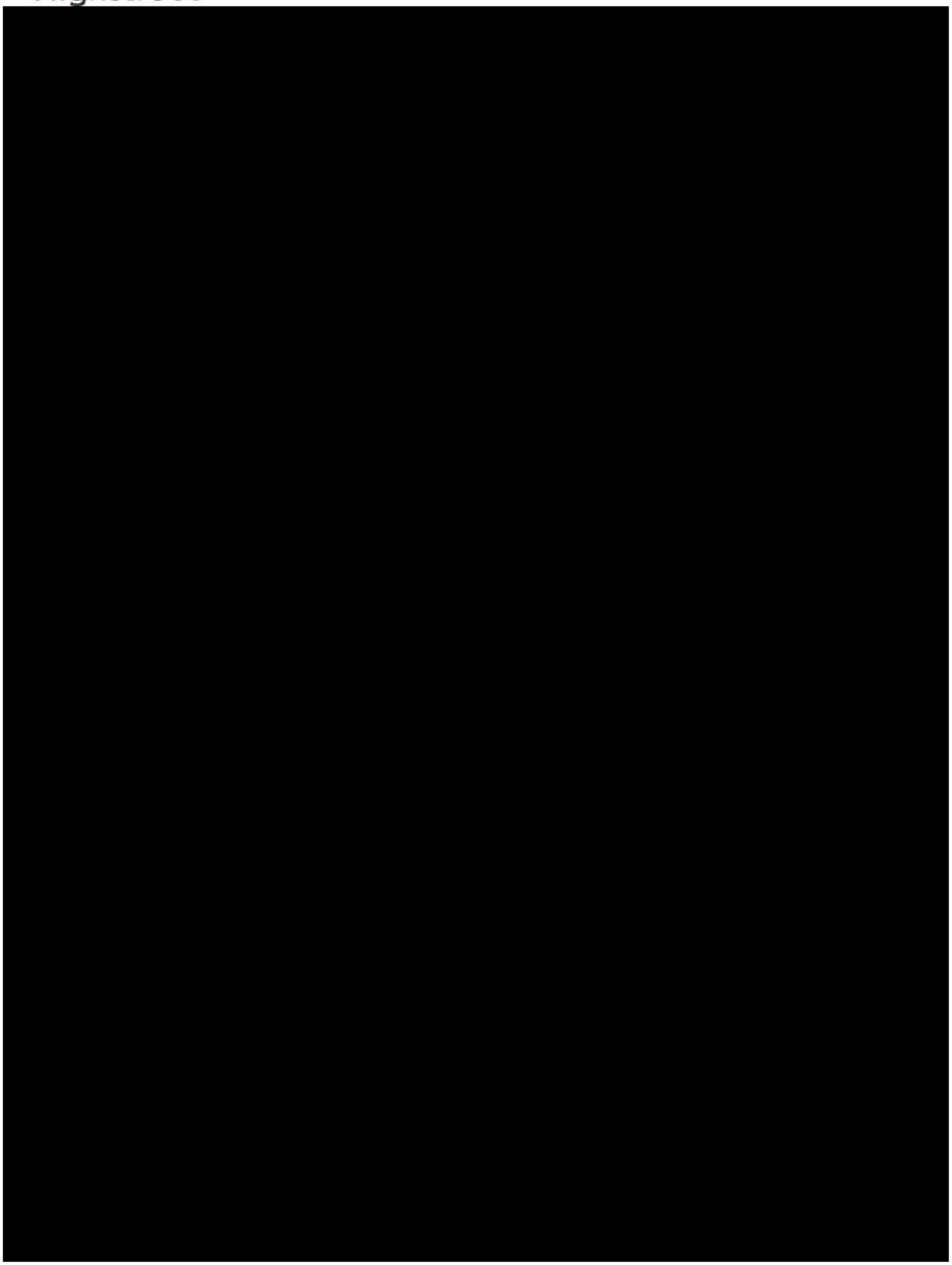
Highstreet does not access customer-specific hardware, operating systems, databases, applications, or any other content located on client hardware unless it obtains formal authorization and approval through a mutually agreed-upon contract.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Highstreet policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Highstreet team member.







Highstreet

Control Activities-Security

Information Security

Highstreet has published security guidelines, approaches, and requirements within its Information Security Policy. Roles and responsibilities for information security are defined within the formal employee job descriptions. Information Security is governed and monitored by a designated member of the Highstreet Management Team. An IT Advisory Board meets on a regular basis to address corporate security concerns and internal policies. The Information Security Policy is reviewed and approved by the IT Advisory Board at least on an annual basis.

Security Policy

The Information Security Policy is enforced through the Employee Handbook which is distributed and acknowledged by employees during the onboarding process. The Information Security Policy is also reviewed during annual security awareness training.

Security Standards

Security standards with regards to mobile computing and communications are a standard part of Highstreet's Security Awareness training program. Highstreet has established an Acceptable Use Policy with rules for the use of mobile devices, email, internet services, and instant messaging. Violations of the Acceptable Use Policy include penalties up to and including termination, based on the outcome of incident investigations. Remote access is controlled through a Virtual Private Network (VPN). Highstreet uses encrypted VPN technology or similar controls for securing remote network connectivity. All wireless devices utilize the WPA encryption protocol. Additionally, the SSID is not broadcast, and all devices have had their default passwords changed.

Highstreet utilizes a third-party entity to scan, detect, assess, and remediate any security vulnerabilities on the network. This software scans the entire network to identify possible security threats and provide recommendations to remediate the identified vulnerabilities.

Physical Security

All Highstreet building facility perimeter and fire exit doors are alarmed, monitored, and tested periodically to ensure operational functionality. The delivery and loading area are also physically separated from the remainder of the Highstreet administrative office. No client environments are contained in Highstreet facilities.

Highstreet maintains a policy requiring all employees, contractors and third-party visitors and vendors to wear a visible identification badge. Security cameras are used to monitor security and compliance at all perimeter doors, as well as to record activities on a 24 x 7 basis to a digital video recorder (that is backed up to read-only media daily and stored in a secure location).

Cybersecurity & Risk Assessment Process

Highstreet's Risk Management program provides definitive guidance on the prescribed measures used to manage cybersecurity-related risk at Highstreet.

Highstreet

Highstreet is committed to protecting its employees, partners, clients, and Highstreet from damaging acts that are intentional or unintentional. An effective cybersecurity program is a team effort involving the participation and support of every Highstreet user who interacts with data and systems. Therefore, it is the responsibility of every user to conduct their activities accordingly to reduce risk across the enterprise. IT Risk is assessed as part of Highstreet Advisory Board Meetings on at least an annual basis.

Access Controls

Highstreet maintains a distributed Access Control Policy requiring specific actions before access can be granted to information systems. The access rules and rights for each user and group are documented and communicated to all new employees. Access rights are granted on a need-to-know basis.

Highstreet utilizes a formal process for user registration and de-registration for the granting and revoking of access rights to all information systems and services, and all access requires managerial pre-approval. Highstreet Management conducts a review of access controls for all types of users every six months. User Access rights are also removed or disabled after a period of inactivity.

A formal termination process exists to ensure the proper return of all previously issued corporate assets under the control of the employee (or a third party) and the termination of all accounts.

Highstreet maintains a complex password policy for its systems and servers. Passwords are stored in an encrypted format on the system and are separate from system data. Users are required to terminate their session when finished, even if they are still in their respective work area. Workstations are also configured to logo off after a period of inactivity.

Anti-Virus Software

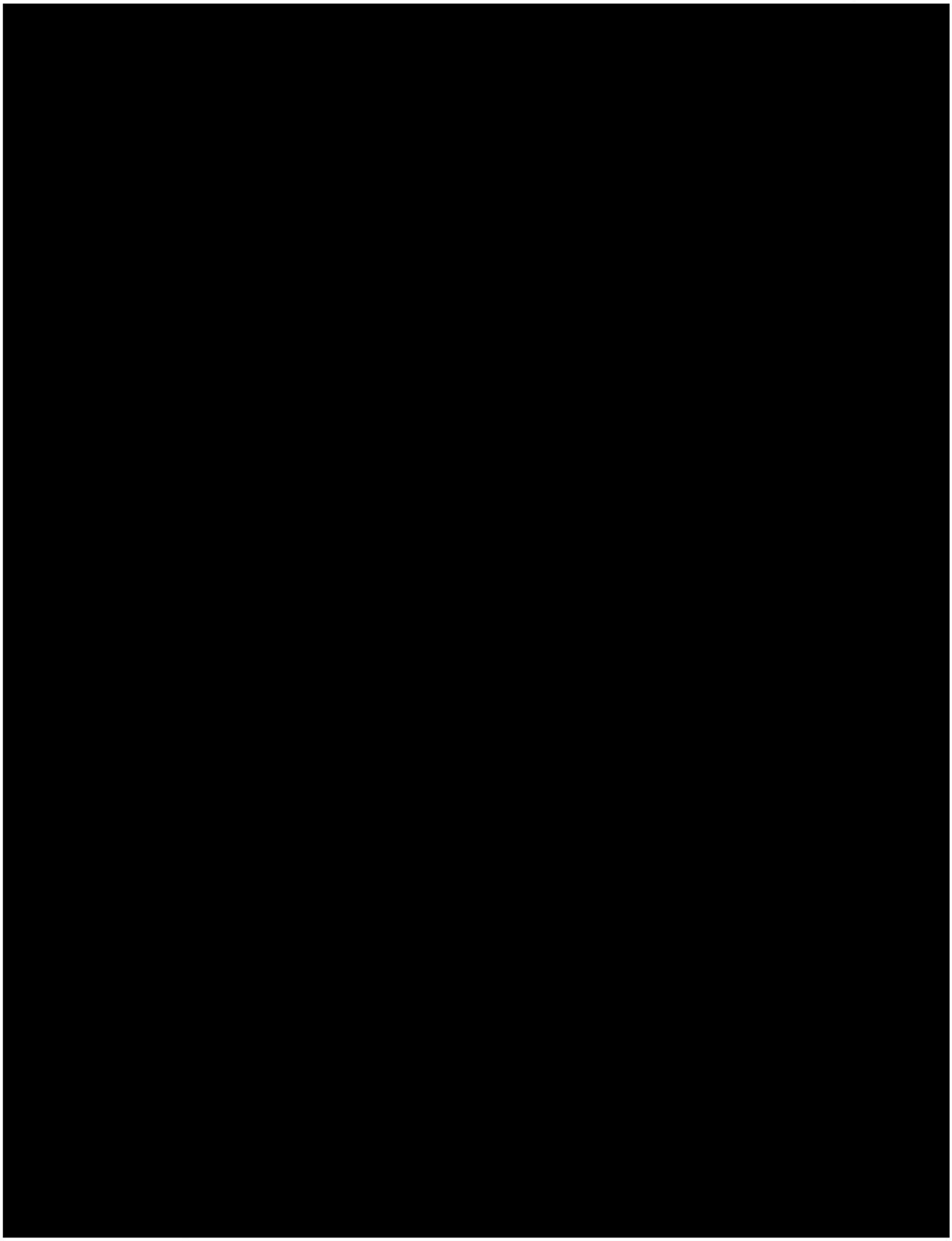
Antivirus software is installed on workstations, laptops, and servers supporting such software. Anti-virus rules are updated as needed.

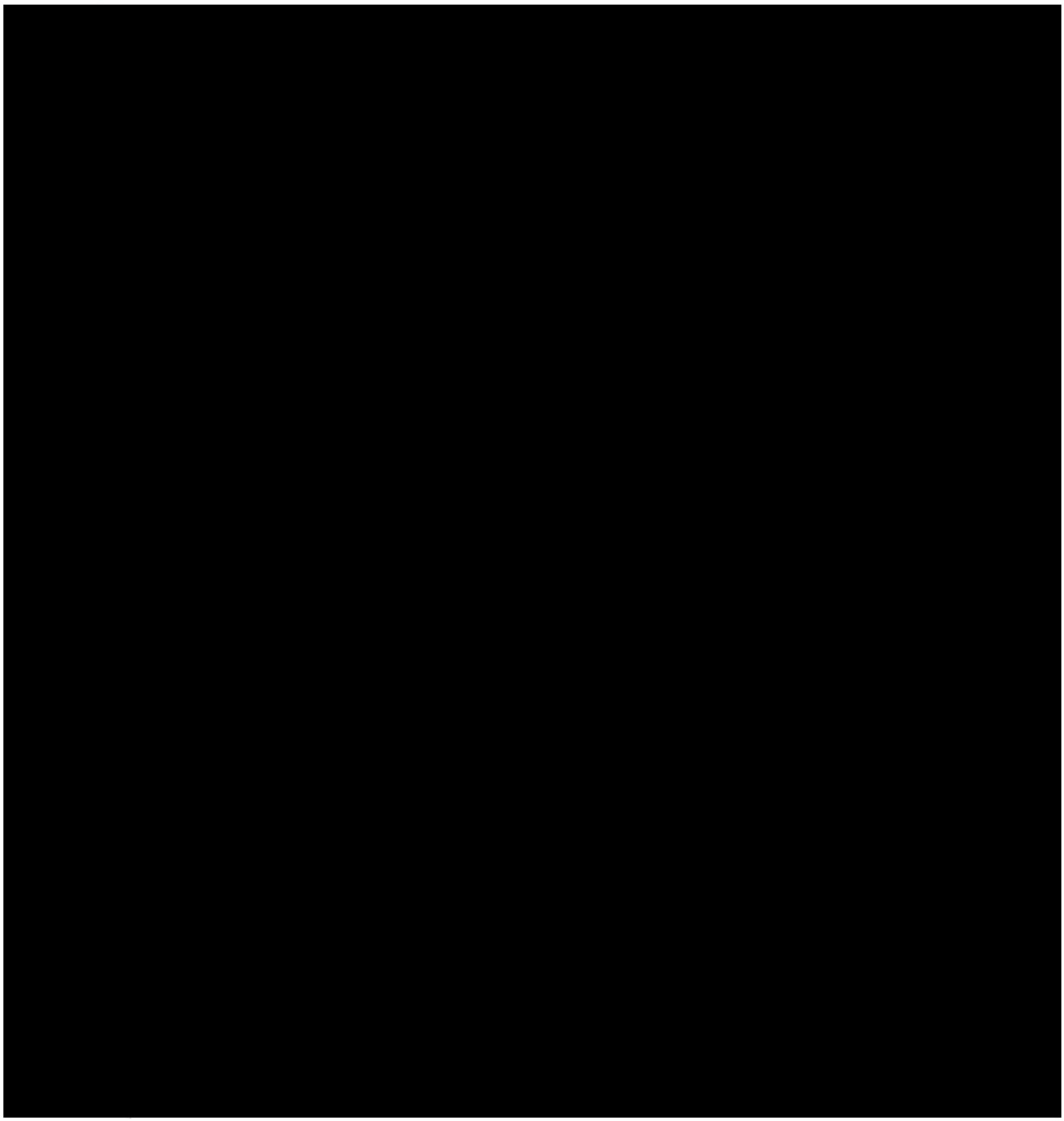
Information Security Monitoring and Incident Management

Highstreet has established a formal incident reporting process in the Information Security Policy, which documents escalation plans and procedures to quickly report information security incidents. Employees, contractors and third parties are required to note and report any observed or suspected security weaknesses in information systems or services to the Information Technology and Security Department. Security incidents are recorded and tracked centrally by the Information Technology and Security Department.

The procedure for the reporting of information security incidents is also a standard part of Information Security Awareness training for all users. There is also a documented formal disciplinary process defined in the Employee Handbook for users who commit security breaches.

Highstreet operations staff actively monitor the intrusion detection system for possible intrusions on a 24/7 basis. Upon detection of any suspicious activity, an investigation and analysis of the possible causes is conducted. Should Highstreet determine that there is a possible hacker attack; the incident handling process will be activated. Failed authentication alerts are also monitored. If the number of invalid user logon attempts are exceeded, the system administrators will be alerted and follow-up as to the potential cause.





Control Activities - Confidentiality

The Company classifies and labels confidential information to ensure appropriate handling and protection. Access to confidential information is restricted to authorized personnel based on role and business need.

The following are in place and followed for Confidentiality:

- Non-disclosure agreements (NDA's) are executed with all contractors prior to granting access to confidential information.
- Non-disclosure agreements (NDA's) are required from all third-party service providers handling confidential information.
- Confidential information transmitted externally is encrypted using industry-standard protocols.
- Confidential information is securely disposed of (e.g., shredding, secure wiping) once it is no longer required for business purposes.

Information & Communication

Highstreet Management reviews its policies, procedures, and standards periodically (and at a minimum, annually) to reflect changing business conditions. A formal annual compliance assessment is performed by Highstreet's Advisory Board, whereby key business processes are reviewed, and exceptions are documented. This assessment includes identifying the root cause, the remedial action required and tracking remediation actions to completion.

Boundaries of the System

The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. Highstreet provides Network, Application, and Cloud Services to its customers. The boundaries of Highstreets System include software and infrastructure that directly support the Network, Application, and Cloud Services provided to customers.

Monitoring Controls

The Advisory Board is comprised of Senior Management and regularly provides information about the functioning of internal controls at Highstreet. Ongoing monitoring activities are also built into the normal activities performed at Highstreet.

Changes to the System During the Period

There were no changes that affect the users of this report's understanding of how the Highstreet's System is used to provide Network, Application and Cloud Services during the examination period from October 1, 2024, to September 30, 2025.

Criteria Not Applicable to the System

The Privacy Trust Services Criteria were not applicable to the services provided by Highstreet. Additional Criteria for Processing Integrity was deemed to be not in scope for this examination. However it is covered in Control C7.02.

Highstreet

Information Security Incidents

To Management's knowledge, there were no system incidents during the examination period from October 1, 2024, to September 30, 2025, which were the result of controls that were not suitably designed. There were no incidents noted during the examination period from October 1, 2024, to September 30, 2025, which resulted in a significant failure in the achievement of one or more of the Company's service commitments or system requirements.

Complementary Subservice Organization Controls

Complementary subservice organization controls (CSOCs) are controls that Highstreet management assumed, in the design of the system, would be implemented by their subservice organizations and are necessary, in combination with controls at Highstreet, to provide reasonable assurance that Highstreet's service commitments and system requirements were achieved.

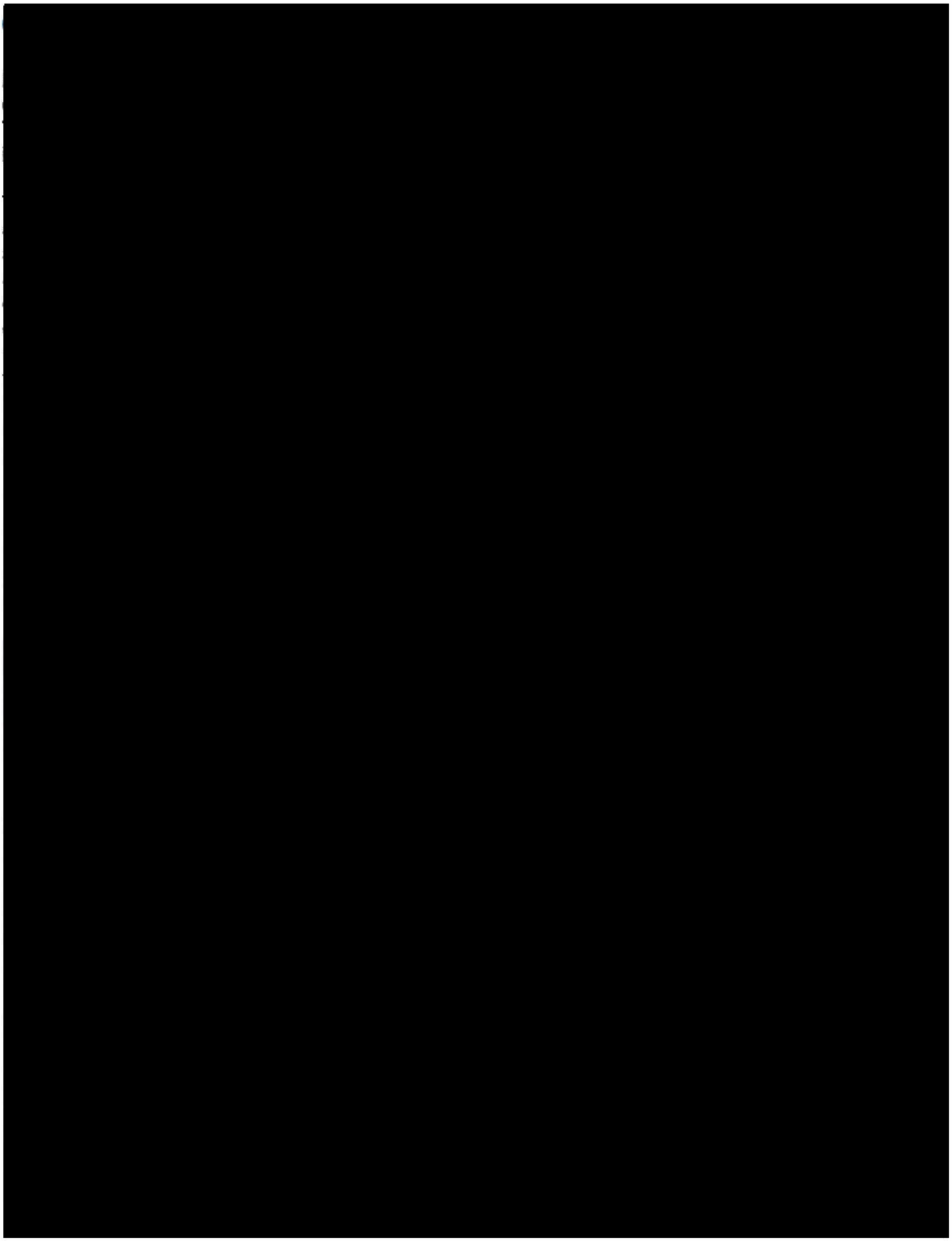
Highstreet uses Subservice Organizations [redacted] to support Highstreet's System. The Subservice Organizations are subject to the same oversight and governance as outlined in the "Description of Highstreet's Network and Application Solutions and Cloud Services System" section previously described. Additionally, various business unit personnel supporting the services within this Description interact with Subservice organization personnel on a regular basis. Highstreet's related service commitments and system requirements can be achieved only if the CSOCs are suitably designed and operating effectively during the period addressed by the description.

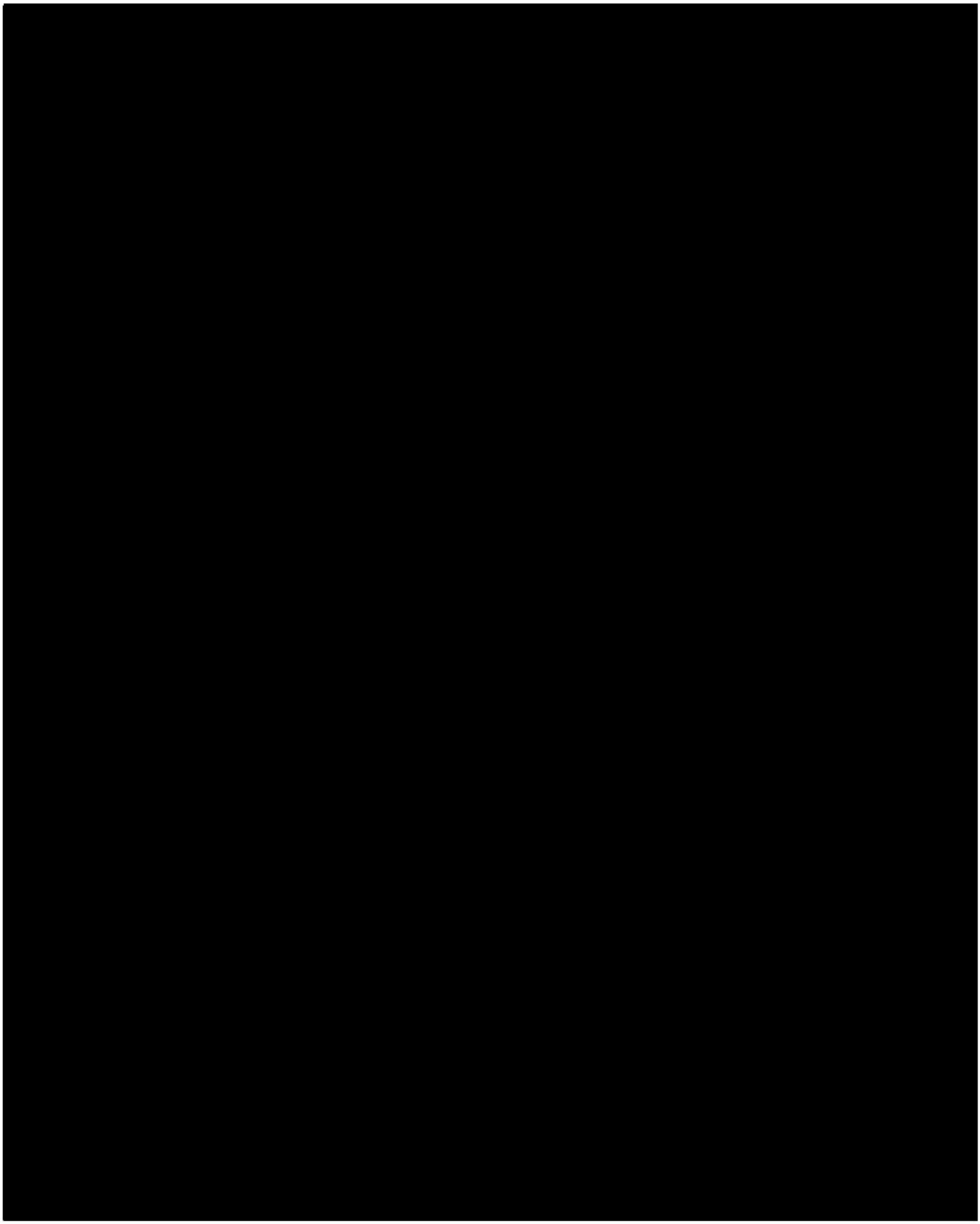
Subservice Organizations have implemented the following key control activities to support Highstreet's Network, Application Solutions and Cloud Services:

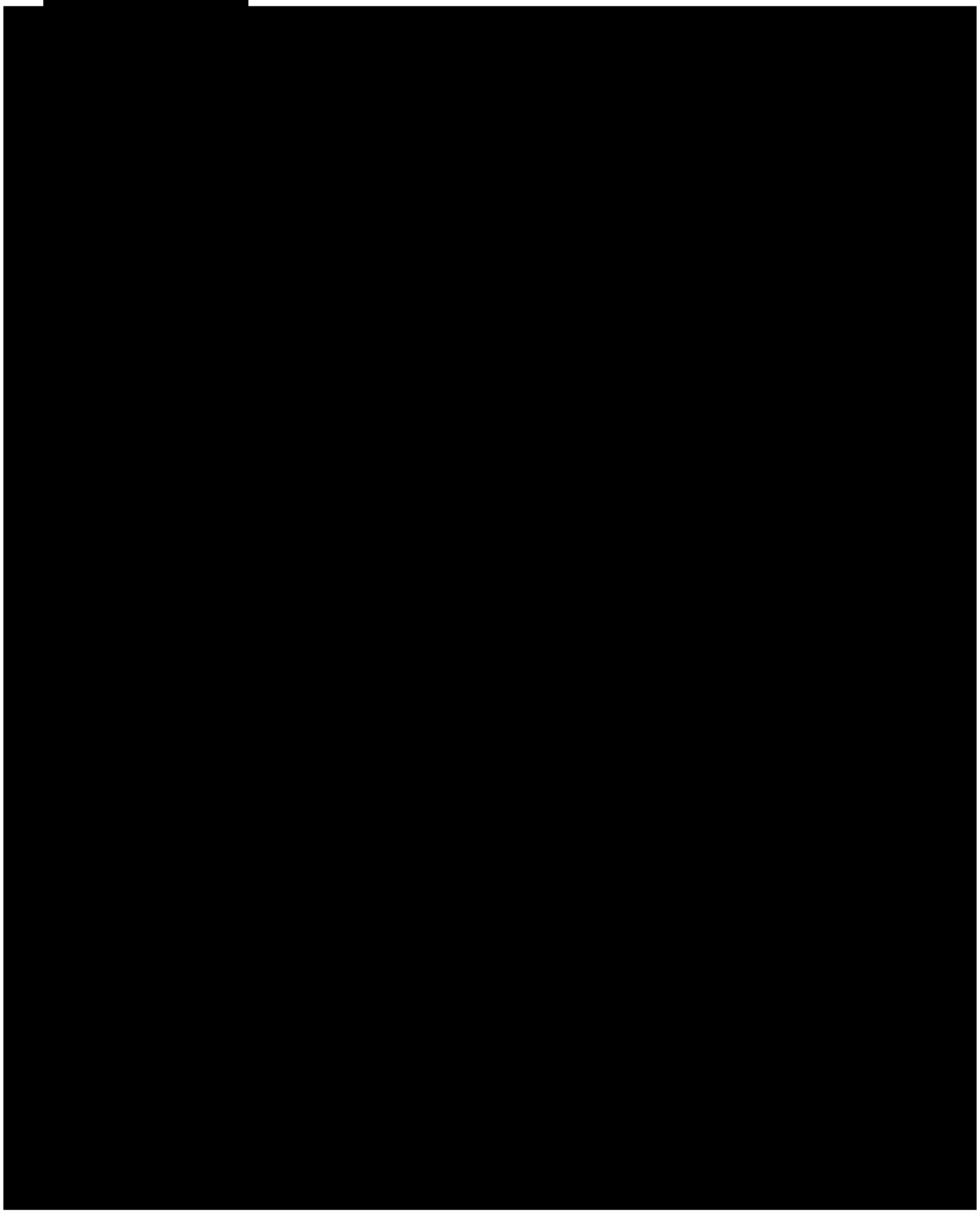
Control Area	Subservice Provider Complimentary Control	Referenced Related Criteria
Security	Controls provide reasonable assurance that information, physical and environmental security policies have been implemented and communicated throughout the organization.	**CC6.0**
Employee User Access	Controls provide reasonable assurance that procedures have been established so that employee user accounts are added, modified, and deleted in a timely manner and reviewed on a periodic basis.	**CC6.0**
Network Security	External points of connectivity are protected by a firewall complex.	**CC6.0**
Incident Monitoring & Reporting	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sends a message to the operations center and automatically opens an incident, problem, or change management "ticket" record when specific predefined thresholds are met.	**CC7.0**

Highstreet

Highstreet reviews Vendor and Service Provider SOC Reports on an annual basis to determine if there are any issues that may affect reliance on the services provided to Highstreet.







Highstreet



Highstreet

Section IV - Highstreet's Security, Availability, Processing Integrity, and Confidentiality Trust Services and Related Controls and Independent Service Auditor's Description of Tests of Controls and Results of Tests

Introduction

This examination was conducted in accordance with the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2 ®).

This section presents the following information provided by Highstreet:

- The relevant Trust Services Criteria and the controls established and specified by Highstreet to meet the relevant Security, Availability, Processing Integrity, and Confidentiality Trust Services Criteria to support that:
    - Security: The system is protected against unauthorized access, use, or modification.
    - Availability: The system is available for operation and use as committed or agreed.
    - Processing Integrity: System processing is complete, accurate, timely and authorized. **NOTE:** Additional Criteria for Processing Integrity is not in scope for this examination, however the Company monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives. **(Refer to Control #7.02).**
    - Confidentiality: The Company enforces a code of ethics and security policies that include confidentiality requirements, communicated through Policy, and reinforced during onboarding and annual training. **NOTE:** Confidentiality Common Criteria are tested in **Controls # 10.01 to 10.06**.

Although the relevant Security, Availability Processing Integrity, and Confidentiality Trust Services Criteria and related controls are presented in Section IV, they are an integral part of Highstreet's Description of its System.

Also included in this section is the following information provided by the independent service auditor, eDelta CPA Services, P.C. ("eDelta"):

- A description of the testing performed by eDelta to determine whether Highstreet's controls were operating with sufficient effectiveness to achieve the relevant security and availability Trust Services Criteria. eDelta determined the nature, timing, and extent of the testing performed.
- The results of eDelta tests of operating effectiveness.

Tests of Operating Effectiveness

The tests applied to determine the operating effectiveness of controls are listed alongside each of the respective control activities within the testing matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the objectives of the applicable Trust Services Criteria were achieved during the examination period. In selecting the tests of controls, eDelta considered the following factors:

- The nature of the control and the frequency with which it operates.
- The control risk is mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.

- The degree to which control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

Types and Descriptions of the Tests of Operating Effectiveness

TYPE	DESCRIPTION
Inquiry	Inquired about appropriate personnel seeking relevant information or representation including: • Knowledge and additional information regarding the policy, procedure; or specific controls. • Corroborating evidence of the policy, procedure, or controls.
Observation	Observed the existence and/or operation of specific controls as represented.
Inspection	Inspected documents and records indicating performance of the controls. This test includes, but is not limited to, the following: • Inspection of management reports to assess whether items were properly monitored, controlled, and resolved on a timely basis. • Inspections of source documentation and authorizations to verify propriety of processed transactions. • Inspection of documents or records for evidence of performance, such as the existence of initials or signatures. • Inspection of systems' documentation, such as operations manuals, flow charts, and job descriptions.

Sampling

eDelta utilized professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. eDelta selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

Test Results

The results of each test applied are listed alongside each respective test applied within the testing matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted" in the test result column of the testing matrices. Any phrase other than the constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the testing matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by user entities and subservice organizations, to complement the control activities and achieve the applicable Trust Services Criteria are presented in the "Complementary User Entity Controls" within Section III.



