UltraViolet Cyber Inc

SYSTEM AND ORGANIZATION CONTROLS

SOC 3 REPORT

Assessment Period: 1st March 2025 to 1st March 2026

Report Validity: 1 Year (1st March 2026 to 1st March 2027)

Issuance Date: 04.08.2026

Management's Report of its Assertions on the Effectiveness of its Controls over Managed Threat Protection Services (System) Based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

TABLE OF CONTENTS

SECTION I ASSERTION OF ULTRAVIOLET CYBER' MANAGEMENT

UVCyber.com

Management Assertion Letter – Ultraviolet Cyber Inc

Management's Assertion Regarding the Effectiveness of Its Controls Over Ultraviolet Cyber Inc Based on the Trust Services Principles and Criteria for Security, Availability, Processing Integrity, and Confidentiality

07-04-2026

We, as management of, Ultraviolet Cyber Inc are responsible for designing, implementing and maintaining effective controls over Ultraviolet Cyber Inc to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means andsophisticated social engineering techniques specifically targeting the entity

We have performed an evaluation of the effectiveness of the controls over the system throughout the period 1st March 2025 to 1st March 2026, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability, processing integrity, and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls wereeffective throughout the period 1st March 2025 to 1st March 2026 to provide reasonable assurance that:

ultraviolet

ultraviolet

UVCyber.com

- the System was protected against unauthorized access, use, or modification to achieve Ultraviolet Cyber Inc's commitments and system requirements
- the System was available for operation and use, to achieve Ultraviolet Cyber Inc's commitments andsystem requirements
- the System processing is complete, valid, accurate, timely, and authorized to achievecommitments and system requirements of Ultraviolet Cyber Inc
- the System information is collected, used, disclosed, and retained to achieve Ultraviolet Cyber Inc's commitments and system requirements based on the Control Criteria.
- Our attached description of the boundaries of Ultraviolet Cyber Inc identifies the aspects of the Ultraviolet Cyber Inc covered by our assertion.

Very truly yours,

Atif Ghauri, President & COO

Ultraviolet Cyber Inc

Virginia (D.C. Area)
1660 International Dr., Suite 600
McLean, VA 22102

Utah
2901 W. Blue Grass Blvd., Suite 200-36
Lehi, UT 84043

India
#3Q, A1, A2, A3, Third Floor, Quadrant No.3, Cyber Towers,
HITEC City, Hyderabad, Telangana 500081 India

ultraviolet

ATTACHMENT A

Description of 'UltraViolet' Services Unified Offensive and Defensive Security Solutions to Security, Availability, Confidentiality, Processing Integrity, and Privacy.

Company Background

UltraViolet Cyber unifies the best defensive and offensive practices to continuously optimize client's security operations. Red and blue-team activities are seamlessly integrated, so you can be confident that as critical and imminent risks are uncovered, vulnerabilities are quickly managed and remediated. The UltraViolet Cyber Security-as-Code platform continuously monitors for threats across complete attack surface, automating investigation and delivering a unified picture of risk to every member of client's security operations team.

UltraViolet' Mission

Our mission is to enable secure, resilient operations so our customers can serve, innovate, and lead with confidence.

Overview of UltraViolet' Services

- Application Security Testing:
  Built for modern development speed, our application security services deliver real-world risk insight and faster remediation.
- Cloud Security Testing:
  Identify and Mitigate Real-World Threats Before They Strike.
- Continuous Penetration Testing:
  UltraViolet Cyber's Continuous Penetration Testing delivers nonstop assessment of your applications, networks, and cloud environments, identifying real attack paths and closing gaps before adversaries strike.
- Continuous Purple Teaming:
  Purple Teaming pairs our offensive operators with your defensive teams in a live, collaborative simulation. Together, we simulate realistic attacks, observe how detections and responses perform, and identify immediate ways to harden your defenses
- Dedicated Défense:
  UltraViolet Cyber's Dedicated Defense embeds certified experts directly into your operations, providing hands-on support, platform management, and continuous reinforcement of your security posture.
- Penetration Testing services:
  UltraViolet Cyber's Continuous Penetration Testing delivers nonstop assessment of your applications, networks, and cloud environments, identifying real attack paths and closing gaps before adversaries strike.
- Red Team Engagements:
  Take an offensive stance against advanced threats with Red Team engagements that simulate real-world, persistent attacks. We go beyond traditional testing to uncover organizational weaknesses, validate detection and response, and provide executive-level insight into your security resilience
- SIEM migration Services:
  UltraViolet Cyber ensures your detections, visibility, and response capabilities stay intact from day one.
- AI Security Services
  UltraViolet Cyber provides security services scross the AI lifecycle, combining strategy, threat modeling, adversarial testing, monitoring, and training to support secure AI adoption
- Managed Detection & Response:
  UltraViolet Cyber's MDR integrates relentless threat hunting with automated response to detect

adversaries fast, contain them in minutes, and deliver measurable resilience across your environment.

- SOC as-a-Service:
  SOC-as-a-Service combines human-led investigation with machine-driven automation to deliver 24x7 monitoring, rapid response, and proven resilience against evolving threats.
- Continuous Threat Exposure Management:
  CTEM delivers continuous vulnerability scanning and risk prioritization across your IT environment, helping you shrink the attack surface and stay audit-ready year-round.
- Vulnerability Management:
  UltraViolet Cyber's CTEM delivers continuous vulnerability scanning and risk prioritization across your IT environment, helping you shrink the attack surface and stay audit-ready year-round.
- Ultraviolet Lens Platform:
  Unified view across detection, response, and offensive testing—turning complex security data into actionable insights so you can prioritize what matters most.
- VOODOO:
  VooDoo toolkit empowers operators to pivot seamlessly across platforms and environments—ARM, macOS, Windows, IoT—enabling deep, collaborative Red Team operations at scale.

Infrastructure:

World-class architecture using industry leading cloud services provider for enhanced performance and business continuity

Application, Software & Tools:

A combination of custom developed, and commercial applications are utilized to support the services provided to user organizations.

System Components

The system is comprised of the following components:

- Infrastructure including the physical structures, information technology (IT) and other hardware.
- Software includes key assets in providing Services offensive and defensive security solutions.

People

Chief Executive Officer
Ira Goldstein: As an entrepreneur and cybersecurity expert, Ira has provided advice on business growth, risk management, and cybersecurity to leaders in both public and private sectors. He is proud to serve as CEO of Ultraviolet Cyber.

President and Chief Operating Officer:
Atif Ghauri: A renowned cybersecurity expert and seasoned professional, Atif Ghauri leads UltraViolet Cyber through an initial growth period and seeks out partnership opportunities across federal and civilian organizations. He is responsible for business strategy, geographic expansion, and service delivery.

Chief Financial Officer:
Lesley Bearg: Lesley leads the Finance organization and serves as a strategic financial thought partner in her role as
Chief Financial Officer. With more than 20 years of experience in Finance as an operator and investment professional, she has a strong track record of building financial teams and sustainably scaling organizations.

Chief Revenue Officer
Wes VanDenburg: Wesley VanDenburg serves as the Chief Revenue Officer at UltraViolet Cyber, where he is responsible for advancing the company's revenue growth by overseeing and aligning all go-to-market functions.
Executive Management: Provides general oversight, and strategic planning and direction.

IT Administrator:
Responsible for software installation/configuration, operations, and maintenance of systems hardware and software relevant to our systems.

Customer Support:
Serves customers by providing product and service information that includes resolving product and service issues.

Audit and Compliance:
Performs regularly scheduled audits relative to defined policies, procedures, and standards; provides continuous improvement feedback; and assesses legal and regulatory requirements.

Procedures

UltraViolet Cyber Inc has developed, and communicated to its users, a set of policies, processes and procedures to restrict physical, logical and technical access to UltraViolet Cyber Inc's facilities and systems. Important Policies and Procedures are as below:

- Organization's Information Security,
- Acceptable Use,
- Antivirus and Patch Management,
- Backup and Recovery,
- Change Management,
- Asset Management,
- Human Resources and Training,
- Risk Management,
- Incident Management,
- Information Classification,
- Information Exchange,
- Internet Use,
- Logical Access,
- Network Security,
- Organization Chart,

- Physical Security,
- Vulnerability Management, and
- Recurring Control Review Procedure

Standard Operating Procedures are defined across which are primarily used internally to guide UltraViolet Cyber Inc employees to support day-to-day operations. All the teams of UltraViolet Cyber Inc are expected to adhere to UltraViolet Cyber Inc policies and procedures that define how the services should be delivered, these are located within the organization's SharePoint/intranet portal and accessible to an authorized user.

Data

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured and utilized by Ultraviolet Cyber Inc in delivering its technological solutions.

Ultraviolet Cyber Inc Access Control Policy applies to all offices and branches of the company, all staff and volunteers of the company and all contractors, suppliers, and other people working on behalf of Ultraviolet Cyber Inc. It applies to all data that the company holds relating to identifiable individuals.
Ultraviolet Cyber Inc processes data for the purposes of reporting, tracking, monitoring etc. of the activity of individuals.

When data is stored electronically, it is protected from unauthorized access, accidental deletion, and malicious hacking attempts. If data is stored on removable media/external storage, these are kept locked away securely when not being used, and only accessible with access credentials.
Passwords for any storage medium or sub-processor are changed regularly. All data is monitored in real-time, providing notification of unusual activity.

Relevant Aspects of Control Environment, Risk Assessment, Information and Communication, Monitoring Activities, and Control Activities

Control Environment

Integrity and Ethical Values

Passion

We make sure to live with passion and create an environment where our team feels appreciated and valued. We strive for a passionate environment at work and never stop learning.

Innovation

We are solution oriented to make today better! Use out of the box ideas, technology and solutions to make today better for our clients and our company. We are problem solvers who relentlessly innovate and plan for long-term and scalable solutions to solve the security challenges of today and tomorrow.

Trust

We respect differences of opinion and experiences and collaborate in an open sharing environment to establish and maintain trust in your community.

A Will to Win

We relentlessly strive to win for our community, win for our clients, and win against the adversary.

Inclusion

We create a community that fosters inclusiveness, diversity and equity to all.

Organization Structure & Assignment of Authority and Responsibility

UltraViolet Cyber Inc employs a management team consisting of C-Level leadership in all functional areas. This group reports to the COO / President and, in turn, the CEO. Each functional area is predominantly structured in a hierarchical manner with layers of management employed as appropriate based on organization size, specialization, and duties. Organizational charts are in place to communicate areas of authority, responsibility, and the lines of reporting to personnel.

Commitment to Competence

UltraViolet Cyber Inc's management defines competence as skills that are required to deliver the assigned tasks that define employee roles and responsibilities. Commitment to competence includes management's consideration of competence levels for particular jobs and how those levels translate into required skills and knowledge. UltraViolet Cyber Inc has written job descriptions specifying the responsibilities for job positions. Job descriptions are periodically reviewed and updated as necessary. Technical training is provided to employees to expand the knowledge base and improve performance.

Information Security

UltraViolet Cyber Inc has a formal information security protection program based on ISO 27001: 2022 framework and periodically certifies its compliance with the standards. The information security policy is formally documented, actively monitored, reviewed, and updated to ensure its objectives continue to be met.

An organizational structure is defined for information security which details the reporting lines, authorities, and responsibilities for business operations. The roles and responsibilities of the members of the information security organization are defined. Information Security Policy and information security-related procedural documents for processes are made available to the employees.

Training and Awareness

An information security education and awareness program has been established that includes policy training and periodic security updates to UltraViolet Cyber Inc's personnel. New hires and existing employees are required to undergo Information Security Awareness Training via a training portal.

Information security related policies and procedures are communicated to the employees during the induction training and are made accessible to employees via SharePoint. Personnel using mobile computing devices/teleworking are trained on the risks, the controls implemented, and their responsibilities.

UltraViolet Cyber Inc has developed, implemented, and maintained a comprehensive privacy protection awareness and training program to educate relevant personnel on their responsibilities of protecting PII and organizational procedures. Also, modules related to privacy protection and awareness are also covered during the Information Security training conducted for all employees.

The training focused on the technology domain, soft-skills, and behavior are conducted periodically for employees as part of the learning and capabilities development initiatives of the organization.

Human Resources Policies and Procedures

UltraViolet Cyber Inc maintains written Human Resources Policies and Procedures. The policies and procedures describe UltraViolet Cyber Inc practices related to hiring, learning and development, performance reviews and advancement, code of conduct, disciplinary action, and termination. Employee candidates' ability to meet job requirements is evaluated as part of the hiring evaluation process.

Competency metric exists that defines the competency requirement for every role, the recruitments are carried out based on this. UltraViolet Cyber Inc requires employees to provide their acceptance on the offer letter that includes employment terms and conditions.

In addition, new joiners are required to sign a 'Non-Disclosure Agreement' at the time of joining. Third party background verification check is conducted for all employees joining UltraViolet Cyber Inc. All employees are required to authorize a background check by signing a consent form.

Annual performance evaluation is conducted via performance management process where employees are evaluated based on the performance criteria and organizational values. UltraViolet Cyber Inc has documented Anti-Harassment Policy to maintain a workplace free of harassment. Awareness training is conducted periodically.

Information and Communication

UltraViolet Cyber Inc utilizes various methods of communication to help ensure employees understand their roles and responsibilities and the entity's controls. UltraViolet Cyber Inc's knowledgebase is hosted on their intranet portal to disseminate information to employees. UltraViolet Cyber Inc has established various communication channels to communicate with external stakeholders. UltraViolet Cyber Inc provides periodic reporting on operations and other relevant reports as agreed with the clients.

Risk Assessment and Risk Treatment

Risk Assessment and Treatment Procedure is documented to assess risks of information assets and services as per the context stated in the Information Security policy and ISMS Manual. Risk assessment is performed at least annually by GRC/Compliance team but may be performed more often in case of any changes to the technical or business landscape or other changes that introduces new risk to the organization to identify and manage risk across UltraViolet Cyber Inc. Privacy risk assessment is performed on an annual basis by the GRC/Compliance team to identify, assess, and mitigate privacy risks.

Monitoring Activities

UltraViolet Cyber Inc performs periodic Information Security Management System (ISMS)/Service Management System (SMS) reviews and results are reviewed with management. This involves monitoring ongoing effectiveness and improvement of the control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.

UltraViolet Cyber Inc undergoes ISO 27001 independent audit at least annually, to monitor and verify compliance with security and service management system requirements. The findings are recorded, reviewed, prioritized, and remediation plans are developed.

Internal audits are performed twice a year as per the Internal Audit Policy & Procedure and effectiveness is documented in the form of the Internal Audit Summary and discussed during the management review meetings. Audit Findings are recorded as a part of CAPA (Corrective Action & Preventive Action), and remediation is tracked in the tool by the GRC/Compliance team.

Control Activities

Access Administration
Access to the customer's information by UltraViolet Cyber Inc employees is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances.

Access Control Policy is formally documented, reviewed, and approved at least on an annual basis. User registration and de-registration formally address establishing, activating, modifying, reviewing, disabling, and removing accounts. Logical access to UltraViolet Cyber Inc' systems is restricted through Active Directory based domain policies. UltraViolet Cyber Inc maintains administrative safeguards for the protection of confidentiality and integrity of customer data.

Password Management
There is a defined password policy specifying minimum password length, maximum password age, password complexity requirement, and account lockout.

The organization's password requirements are documented in Access Control Policy (IT POLICIES AND PROCEDURES) published, communicated, and made available to all employees via SharePoint. In-scope system components require a unique username and password before authenticating users.

Before deploying any new devices in a network environment, the organization changes all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

Network Security
Firewalls are implemented and configured to protect the network from external threats and vulnerabilities. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.

Access to the internet is controlled and monitored through content filtering settings configured in the firewall. All production application servers are hosted behind a WAF to prevent common attack traffic. The IT team is notified of suspicious activity through alerts received from Palo Alto. Alerts are addressed promptly based on the severity. Firewall rules are reviewed bi-annually.

There is no direct connection between the internal network and the internet, all connections to the internet from the internal network are through firewalls. All the connections to the client network are allowed only after reviewing the requirements by the infrastructure team. Connection to the client network is always encrypted and wherever possible UltraViolet Cyber Inc insists on two factor authentication.

Remote access to UltraViolet Cyber Inc's network by authorized employees is through VPN connection. Multi-factor authentication is implemented for remote connectivity. Access to AWS instances for ports other than 80 and 443 are allowed only from UltraViolet Cyber Inc' corporate network.

Endpoint Protection

There exists a documented Antivirus Policy for antivirus management and monitoring. UltraViolet Cyber Inc Endpoint Security is installed on all workstations and on production servers that are in the UltraViolet Cyber Inc's domain. On a monthly basis, the asset list is compared with the reports to verify whether the Endpoint Security solution is installed on all UltraViolet Cyber Inc assets.

Software Installation

End users in SOC Team do not have permissions to install software on the workstations. Software installation requests are submitted to the IT Team via ticketing tool/ email and carried out based on the approval from the respective manager and/ or GRC/Compliance Team.

Encryption and USB Management

Full disk encryption is enabled in all user workstations. USB access is disabled for all users in the SOC Team. USB access is requested via email/ticketing tool and approved on the business justification. Approved list of devices and users are maintained by the GRC/Compliance Team.

Security Configuration

The Infrastructure Team is responsible for security configuration as per the industry standard. Information Security Compliance team conducts configuration audits to verify if the servers, workstations, and network devices are configured as per the standard.

Inventory of Assets

UltraViolet Cyber Inc maintains an inventory of hardware and software used in the UltraViolet Cyber Inc network. A list of authorized software is maintained. UltraViolet Cyber Inc ensures outdated software are removed and existing software are fully patched.

Vulnerability Assessment and Penetration Testing

UltraViolet Cyber Inc conducts a periodic vulnerability assessment to identify potential vulnerabilities, then validate and prioritize them based on scores, such as CVSS for all CVE vulnerabilities, and create a prioritized remediation.

SOC Monitoring

SOC monitors changes in critical systems, network devices and workstations. Security logs are monitored 24/7 by UltraViolet Cyber Inc SOC Team. The Critical Observation Report (COR) is published by the SOC team daily to the management and respective teams describing the changes.

The report consists of the below critical activities:

- Threats
- Managed Services like EDR
- Privileged User Monitoring
- Changes to Identity and Access Policies
- Application Activity Monitoring

Change Management

Documented Change Management policies and procedures are in place to guide personnel in change management activities affecting existing IT infrastructure. Infrastructure changes and patches to third party software and applications are tested by the technical support department being applied to production servers.

The IT team is in charge of managing changes to the UltraViolet Cyber Inc infrastructure. All changes are approved by the Delivery Head prior to implementation. The changes are recorded and tracked to closure by the IT team. All changes to the infrastructure are discussed during the monthly staff meetings.

Patch Management

UltraViolet Cyber Inc has implemented a patch management process to ensure that security updates are patched regularly on servers, network devices and workstations.

The Infrastructure Team ensures that all patches are tested before applying to the production environment. On a monthly basis, the GRC/Compliance Team verifies the application of patches by comparing the patch reports with the asset list.

Information Security Incident Management

An incident management framework has been established and communicated to all employees with defined processes, roles and responsibilities for the detection, escalation, and response of security incidents. Incident Management framework includes the steps of the incident management process and the factors that relate to the whole system.

Business Continuity

Business Continuity Plan is developed to ensure the continuation of the business during and following any critical incident that results in disruption to the normal operation capability. Disaster scenarios, response, and recovery strategies are documented in the Business Continuity Plan.

The plan describes, at a high level, the purpose, objectives, scope, critical dependencies, RTO/RPO, and roles/responsibilities. The mission of UltraViolet Cyber Inc' BCP Team is to help ensure timely recovery of critical business operations of UltraViolet Cyber Inc after a business interruption and return to normalcy.

The Business Continuity Plan is reviewed annually or when there is a material change to the situation. The Business Continuity Plan is tested at least twice a year. After BCP tests are performed, outputs of the tests are captured, analyzed, and discussed to determine the scope of the next steps for continuous improvement

Backup, Replication, and Restoration

UltraViolet Cyber Inc has a documented Backup and Restoration procedure to ensure adequate back-up for recovering essential business information and systems.

Third Party Security Policy

UltraViolet Cyber Inc has established a Third-Party Security Policy. Third-party risks are assessed before signing any contract with third parties and during the annual risk assessment process. Service Contracts along with confidentiality agreements are signed with vendors or third-party providers.

Capacity Management

UltraViolet Cyber Inc has developed and implemented a capacity management process to manage capacity demand. Capacity Planning is done by process owners and process managers and reviewed during the Technology Steering Committee Meetings. Resource & Capacity Management Information System reports are maintained that provide a concise view of the various parameters that are important to the availability of resources for continuous operations. Infrastructure team monitors the critical servers continuously for the resource utilization.

Physical and Environmental Safeguards

Physical Access to UltraViolet Cyber Inc's premises is controlled through the access control system, close circuit television cameras and security desk. Close circuit television cameras are installed at key locations.

Environmental protections have been installed in UltraViolet Cyber Inc's premises and monitored at regular intervals including the following:

- Cooling systems
- Power backup in the event of power failure
- Redundant communications lines
- Smoke detectors
- Fire Extinguishers

Privacy

UltraViolet Cyber Inc's privacy policy is published on its corporate web portal in clear and conspicuous language. UltraViolet Cyber Inc uses personal information only for the sole purpose of providing the services as specified in the contractual agreement and privacy policy.

UltraViolet Cyber Inc has developed, implemented, and maintained a comprehensive privacy protection awareness and training program to educate relevant personnel on their responsibilities of protecting PII and organizational procedures. Also, modules related to privacy protection and awareness are also covered during the Information Security training conducted for all employees. UltraViolet Cyber Inc performs ongoing procedures for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.

ultraviolet

ATTACHMENT B

Principal Service Commitments and System Requirements

UltraViolet Cyber Inc makes service commitments to its customers and has established system requirements as part of the Managed Threat Protection Services. UltraViolet Cyber Inc is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that UltraViolet Cyber Inc's service commitments and system requirements are achieved.

The principal service commitments are communicated via customer contracts/service level agreement, description of service offering provided online, Information Security Management System (ISMS policy), Service Management System (SMS policy).

UltraViolet Cyber Inc has made commitments to customers with regards to service levels objectives. This involves meeting or exceeding the established SLOs, ensuring that the quality of service provided is consistent and reliable, and addressing any issues or problems that arise promptly and effectively. In order to ensure that SLOs are met, and commitments are fulfilled, UltraViolet Cyber Inc has implemented processes and procedures that monitor and measure the performance of their services and take corrective action when necessary.

UltraViolet Cyber Inc has made commitments related to protecting the information and systems and complying with relevant laws and regulations. These commitments are addressed through measures including encryption, authentication mechanisms, physical security, and other relevant security controls.

UltraViolet Cyber Inc's management establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated to UltraViolet Cyber Inc' system policies and procedures, system design documentation, and contracts with customers.

Information Security Management System policy (ISMS policy) is a document with high-level requirements for establishing an Information Security Management System in UltraViolet Cyber Inc and demonstrate compliance to ISO 27001: 2022.

It also guides the Information Security Steering Committee, Information Security Officer, Information Security Coordinators, Internal/External consultants, and ISMS users in understanding, implementing, maintaining, and reviewing the required security controls. It also clearly defines the authorities and responsibilities and defines overall direction and policies regarding Information Security. It also assesses and addresses the information risks concerning operational activities, infrastructure, and projects the objective of the ISMS is to support the corporate mission regardless of geographic location. UltraViolet Cyber Inc is committed to providing secure networks and systems that protect the confidentiality, integrity, and availability of information and data that the organization uses and/or is entrusted with.

Service Management System (SMS Policy) is to provide the highest level of service to UltraViolet Cyber Inc' customers and ensure that UltraViolet Cyber Inc continually improves the delivery of services to customers.

SECTION II INDEPENDENT SERVICE AUDITOR'S REPORT

P & G ASSOCIATES, PLLC
Public Accounting Firm (FRM)

Regd. Office Address:
1500 N Grant ST, STE B
Denver, CO 80203 USA

Mailing Office Address:
4512 Legacy Drive, Ste 100, Plano,
TX 75024, USA

Tel: +1 (469) 588 5250
Email: info@pandgassoc.com
Regn. No: FRN.5000066

APPENDIX A: GLOSSARY

Independent Service Auditor's Report

To: Management of UltraViolet Cyber Inc

Scope of SOC Audit

We have examined UltraViolet Cyber Inc management's assertion related to 'Offensive Security Services and Defensive Security Services' and Related Services System that, during the period 1st March 2025 to 1st March 2026, UltraViolet Cyber Inc maintained effective controls to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification;
- the system was available for operation and use as committed or agreed.
- the system processing was complete, accurate, timely and authorized;
- Personal information is collected, used, retained, disclosed and destroyed in conformity with the service commitments.
- information designated as confidential was protected by the systems as committed or agreed

based on the criteria for security, availability, processing integrity and confidentiality in the AICPA's 2016 TSP section 100A, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of UltraViolet Cyber Inc's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of UltraViolet Cyber Inc's relevant controls over security, availability, processing integrity and confidentiality (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

The description indicates that UltraViolet Cyber Inc's controls can provide reasonable assurance that certain service commitments and system requirements relating to applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of UltraViolet Cyber Inc's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.
As indicated in the description, UltraViolet Cyber Inc uses subservice organizations for providing customer services. The description in Section 3 includes only the controls of UltraViolet Cyber Inc and excludes controls of the various subservice organizations. The description also indicates that certain trust services criteria can be met only if the subservice organization's controls, contemplated in the design of UltraViolet Cyber Inc's controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to controls of various subservice organizations for data center services.

Service organization's responsibilities

UltraViolet Cyber Inc is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved.

UltraViolet Cyber Inc has provided the accompanying assertion titled, Management of UltraViolet Cyber Inc's Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirement would be achieved based on the applicable trust services criteria if operating effectively. UltraViolet Cyber Inc is responsible for (1) preparing the Description and Assertion;

(2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the description based on the description criteria set forth in UltraViolet Cyber Inc's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is presented in accordance with the description criteria and (2) the controls are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements relating to applicable trust services criteria stated in the description would be achieved throughout the period 1st March 2025 to 1st March 2026.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Service Auditor's Independence and Ethical Requirements

We have complied with the independence requirements and other ethical responsibilities in accordance with relevant ethical requirements related to this engagement.

Inherent limitations

Because of the nature and inherent limitations of controls, the UltraViolet Cyber Inc's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct errors or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the systems or controls.

Opinion

In our opinion, UltraViolet Cyber Inc management's assertion referred to above is fairly stated, in all material respects, and UltraViolet Cyber Inc controls over the system operated effectively, based on the aforementioned trust service criteria for security, availability, processing integrity, confidentiality and Privacy.

Mr. Subhajit Guha, CPA
For P&G ASSOCIATES, PLLC
Public Accounting Firm
Firm Registration Number: 5000066

{Remainder of the page left blank intentionally}

P & G ASSOCIATES, PLLC
Public Accounting Firm (FRM)

Regd. Office Address:
1500 N Grant ST, STE B
Denver, CO 80203 USA

Mailing Office Address:
4512 Legacy Drive, Ste 100, Plano,
TX 75024, USA

Tel: +1 (469) 588 5250
Email: info@pandgassoc.com
Regn. No: FRN.5000066

APPENDIX B: ABBREVIATIONS

Abbreviation	Expanded Form
AICPA	American Institute of Certified Public Accountants
ATS	Automatic Transfer Switch
CAB	Change Advisory Board
CEO	Chief Executive Officer
COO	Chief Operating Officer
COR	Critical Observation Report
CPA	Certified Public Accountant
CRAC	Computer Room Air Conditioner
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DC	Description Criteria
HSSD	High Sensitivity Smoke Detection
IP	Internal Protocol
IPS	Intrusion Prevention System
ISC	Information Security and Compliance
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Infrastructure Team
LLC	Limited Liability Company
NDA	Non-Disclosure Agreement
PCI DSS	Payment Card Industry Data Security Standard
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Information Event Management
SLO	Service Level Objectives
SMS	Service Management System
SOC	Security Operations Center
UEBA	User Entity and Behavior Analytics
USB	Universal Serial Bus
VPN	Virtual Private Network
WAF	Web Application Firewall
XDR	Extended Detection and Response

END OF REPORT