PLANET SECURITY

CYBER | ENERGY | WATER

CLIENT NAME

Information Security Policy

Policy Statement

The purpose of this policy is to provide a security framework that will ensure the protection of CLIENT Information from unauthorized access, loss of integrity, and/or compromised availability. CLIENT Information may be verbal, digital, and/or hardcopy, individually controlled or shared, stand-alone, or networked, used for production, administration, research, teaching, or other purposes. Standards and procedures related to this Information Security Policy will be developed and published separately. Failure to comply with this policy may subject you to disciplinary action up to and including termination of the person in violation.

Who is Affected by This Policy

The Information Security Policy applies to all CLIENT employees or contractors with employee-like access. This policy also applies to all other individuals and entities granted use of CLIENT Information, including, but not limited to, interns, temporary employees, and volunteers.

Controlled Unclassified Information (CUI)

CUI is an identified level of value for information. When information has been identified as CUI, it must be protected to the criteria outlined and in the DFARS 252.204-7012 and detailed in the NIST SP800-171r2. CUI within the CLIENT organization is to be exclusively housed within the CPE/SPE environment.

This Environment includes:

- The CPE/SPE Server and its subcomponents
- Any additional workstations which have been contractually attached to the CPE/SPE environment for additional functionality.
- Any network attached printers/MFC/ or other devices which are contractually attached to the CPE/SPE environment.
- Any USB attached devices provided with the CPE/SPE (Backup HDD, Flash Media, etc)
- Any production equipment used to perform actions in the making of a covered item (CnC, other operational technology). These devices shall never be used to persistently house CUI. Once the job is finished, the information is to be removed from the operational device.

These are the ONLY locations approved for logical CUI.

Physical (Paper or other) media containing CUI shall be printed/created only when necessary in the performance of official duties related to the satisfaction of a contract. Physical CUI asset's CONFIDENTIALITY must be assured as per the aforementioned references requirements. Procedures for Creating, Maintaining, Usage, and Destruction of physical CUI assets are identified in procedure: PRO.CUI.COMPLETE.

The details contained in the aforementioned procedure reflect the ONLY locations, methods, and reasoning pertaining to Physical CUI.

Additional Definitions

Authorization – the function of establishing an individual's privilege levels to access and/or handle information.

Availability – ensuring that information is ready and suitable for use.

Confidentiality – ensuring that information is kept in strict privacy.

Integrity – ensuring the accuracy, completeness, and consistency of information.

Unauthorized access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.

CLIENT Information – information that CLIENT collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

Policy Structure

This information security policy contains the following sections.

- Access Control (AC) 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21
- Awareness and Training (AT) 1 | 2 | 3
- Audit and Accountability (AU) 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
- Configuration Management (CM) 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
- Identification and Authentication (IA) 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11
- Incident Response (IR) 1 | 2 | 3
- Maintenance (MA) 1 | 2 | 3 | 4 | 5 | 6
- Media Protection (MP) 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
- Personnel Security (PS) 1 | 2
- Physical Protection (PE) 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10
- Risk Assessment (RA) 1 | 2 | 3
- Security Assessment (CA) 1 | 2 | 3 | 4
- Systems and Communications Protection (SC) 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17
- System and Information Integrity (SI) 1 | 2 | 3 | 4 | 5 | 6 | 7

Access Control

POL.AC.L1-3.1.1

All CLIENT information systems that store, process, or transmit CUI shall employ Role Based Access Control (RBAC) to limit system access to only authorized users of CUI. Furthermore, all processes shall be visible and identifiable to both system administrators and the client user who is logged in (client user respective processes only). All devices which have the capacity to view CUI shall be identified, contractually covered by Planet Security, Inc. The use of shared accounts and/or passwords is prohibited.

All CLIENT non-digital CUI assets shall be protected at all times from confidentiality compromise. All personnel who have access to non-digital CUI assets shall follow Planet Security, Inc. provided procedures pertaining to the same for ensuring confidentiality of non-digital CUI assets. Procedure I.D: PRO.AC.L1-3.1.1

POL.AC.L1-3.1.2

All CLIENT information systems that store, process, or transmit CUI shall employ Application Whitelisting with only approved and authorized applications included in the list. Non-listed applications shall be implicitly blacklisted.

POL.AC.L1-3.1.20

All CLIENT information systems that store, process, or transmit CUI shall only allow external system connectivity:

- From approved Remote Desktop Protocol (RDP) Client Devices
- To Signal Messenger systems and other connected Signal Users
- Web browsing via Brave web browser to allowed websites. No attempt to access non-approved websites shall be made.
- All other connections to external systems are prohibited.

POL.AC.L1-3.1.22

CUI shall never be posted, published, or otherwise be allowed to be housed on any publicly accessible information system or any other system that has not been explicitly authorized for such usage by this policy.

Violations may include Organizational Termination and Criminal prosecution as authorities may pursue.

POL.AC.L2-3.1.3

CLIENT management shall only approve access to CUI to those who NEED such access in the performance of their assigned duties. This pertains to both digital and non-digital CUI assets.

POL.AC.L2-3.1.4

All CLIENT employees, or contractors with employee-like access shall be aligned in such a manner as to promote security through the inability to perform malevolent activity without collusion.

POL.AC.L2-3.1.5

All CLIENT information systems shall employ the principle of least privilege. No employee, contractor, or representative of CLIENT shall have access to security functions or privileged accounts. Elevated access of any CPE/SPE environment is the sole responsibility of Planet Security, Inc.

POL.AC.L2-3.1.6

CLIENT personnel shall not have elevated provisioning at any time. Planet Security, Inc. personnel shall not have access to any form of CUI.

POL.AC.L2-3.1.7

CLIENT personnel shall not have the ability to execute privileged functions. Privileged execution attempts shall be logged, both success and failure.

POL.AC.L2-3.1.8

Unsuccessful logon attempts shall be limited to 5 on any system that stores, processes, or transmits CUI.

POL.AC.L2-3.1.9

Privacy and security notices consistent with applicable CUI rules shall be presented to the the logging-in user on any system that may store, process, or transmit CUI.

POL.AC.L2-3.1.10

Session lock with pattern-hiding displays to prevent access and viewing of data after 15 minutes of inactivity on any system that may store, process, or transmit CUI.

POL.AC.L2-3.1.11

User sessions shall be terminated after 120 minutes of inactivity on any system that may store, process, or transmit CUI..

POL.AC.L2-3.1.12

Any system that may store, process, or transmit CUI shall monitor and control remote access sessions.

The exclusive method of remote access sessions for any system that may store, process, or transmit CUI shall be RDP sessions that originate from an approved white-listed IP address. Remote access shall be limited to IP address spaces within the United States of America.

POL.AC.L2-3.1.13

Any system that may store, process, or transmit CUI shall exclusively employ FIPS algorithms and cryptographic modules when used to to protect the confidentiality of CUI usage within remote access sessions.

POL.AC.L2-3.1.14

Remote access shall be via a single entry point on the CPE/SPE.

POL.AC.L2-3.1.15

Security-relevant information shall only be available to Planet Security, Inc.

POL.AC.L2-3.1.16

Wireless connectivity shall not be used to access any system that may store, process, or transmit CUI.

POL.AC.L2-3.1.17

Wireless connectivity shall not be used to access any system that may store, process, or transmit CUI.

POL.AC.L2-3.1.18

Wireless connectivity shall not be used to access any system that may store, process, or transmit CUI.

POL.AC.L2-3.1.19

Authorized mobile devices and/or mobile computing platforms that store, process, or transmit CUI shall utilize FIPS validated full drive encryption. Exclusive RDP access from these devices does not necessitate the encryption of these devices.

POL.AC.L2-3.1.21

Use of Portable media devices shall be exclusively:

- Be limited to the two portable hard drives which are/were supplied with the CPE/SPE for backup purposes.
- Be limited to the two USB "Thumb Drives" which are/were supplied with the CPE/SPE for purposes of transferring digital CUI assets to CLIENT operational technology devices such as manufacturing devices (CNC, other).
- The aforementioned devices shall never be plugged in or otherwise used in any non-CLIENT device or the CPE/SPE.

Awareness and Training

POL.AT.L2-3.2.1

As part of new-hire orientation, annual refresher training, or when a significant change in the environment occurs, all users who have access to CUI are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

POL.AT.L2-3.2.2

As part of new-hire orientation, annual refresher training, or when a significant change in the environment occurs, all users who have access to CUI are trained to carry out their assigned information security-related duties and responsibilities.

POL.AT.L2-3.2.3

As part of new-hire orientation, annual refresher training, or when a significant change in the environment occurs, all users within the organization, regardless of CUI access shall be trained on recognizing and reporting potential indicators of insider threat.

Audit and Accountability

POL.AU.L2-3.3.1

All systems that store, process, or transmit CUI shall create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Audit logs shall be retained for 90 days.

POL.AU.L2-3.3.2

All systems that store, process, or transmit CUI shall provide non-repudiation to ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

POL.AU.L2-3.3.3

All systems that store, process, or transmit CUI logged events shall be reviewed at least daily by Planet Security, Inc. engineers and findings followed up on until an acceptable due care effort has been performed.

POL.AU.L2-3.3.4

All systems that store, process, or transmit CUI shall shall alert Planet Security, Inc. administrators in the event of an audit logging process failure.

POL.AU.L2-3.3.5

All systems that store, process, or transmit CUI shall transmit log data to the Planet Security, inc. Security Information Event Management (SIEM) tool whereby it may be processed to correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

POL.AU.L2-3.3.6

All systems that store, process, or transmit CUI shall transmit log data to the Planet Security, inc. Security Information Event Management (SIEM) tool whereby audit record reduction and report generation to support on-demand analysis and reporting may be achieved.

POL.AU.L2-3.3.7

All systems that store, process, or transmit CUI shall provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

POL.AU.L2-3.3.8

Audit information and audit logging tools shall be accessible only to Planet Security, Inc. engineers.

POL.AU.L2-3.3.9

Audit logging functionality shall only be made accessible to Planet Security, Inc. engineers who are assigned to support the respective CLIENT organization.

Configuration Management

POL.CM.L2-3.4.1

Baseline configurations and inventories of the CPE/SPE are created and maintained by Planet Security, Inc. for all CLIENT organizations for the entire product life-cycle.

POL.CM.L2-3.4.2

Planet Security, Inc. shall establish and enforce security configuration settings for the CPE/SPE.

POL.CM.L2-3.4.3

Planet Security, Inc. shall track, review, approve, or disapprove, and log changes to the CPE/SPE environment.

CLIENT personnel shall shall track, review, approve or disapprove, and log changes to organizational operations. This group of members is referred to as the Change Control Board (CCB).

POL.CM.L2-3.4.4

Planet Security, Inc. security subject matter experts shall analyze the security impact of changes prior to implementation into a production system.

CLIENT personnel shall track, review, approve or disapprove, and log changes to organizational operations.

POL.CM.L2-3.4.5

Planet Security, inc. shall define, document, approve, and enforce logical access restrictions associated with changes to the CPE/SPE.

Planet Security, inc. shall define, document, approve, and enforce physical and operational access restrictions associated with changes to CLIENT organizational operations.

POL.CM.L2-3.4.6

The CPE/SPE shall employ the principle of least functionality by providing only essential capabilities.

POL.CM.L2-3.4.7

The CPE/SPE shall be configured to restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

POL.CM.L2-3.4.8

The CPE/SPE shall employ and be configured to employ permit-by-exception (whitelisting) policy to allow the execution of authorized software.

POL.CM.L2-3.4.9

The CPE/SPE shall not allow user installed software via Application Whitelisting methodology.

Identification and Authentication

POL.IA.L1-3.5.1

The CPE/SPE identify system users, processes acting on behalf of users, and devices.

POL.IA.L1-3.5.2

The CLIENT shall authenticate (or verify) the identities of users before providing access to CUI.

Planet Security Inc. shall authenticate any process, or device, as a prerequisite to allowing access to CUI.

POL.IA.L2-3.5.3

The CPE/SPE shall utilize MFA for all access, at all times.

POL.IA.L2-3.5.4

The CPE/SPE shall utilize replay-resistant authentication mechanisms for network access to all accounts, at all times.

POL.IA.L2-3.5.5

The CPE/SPE shall never allow the reuse of identifiers (Usernames).

POL.IA.L2-3.5.6

CLIENT shall notify Planet Security, Inc. of anyone who will be out of the office for more than 3 consecutive days via Signal Messenger at least 3 days prior to their absence. Planet Security, Inc. shall disable the account in the CPE/SPE during this time. The account shall be re-enabled upon their return and at the request of the CLIENT.

CLIENT will ensure that all CLIENT organizational personnel are made aware of the respective absence in advance, and will ensure updating of CLIENT personnel upon the return of the subject.

POL.IA.L2-3.5.7

The CPE/SPE shall enforce a minimum password length of 8 characters and shall consist of at least three of the following four complexity classes:

- Upper Case
- Lower Case
- Special Character
- Numerical Value

POL.IA.L2-3.5.8

The CPE/SPE shall prohibit password reuse for twelve (12) generations.

Passwords used for CPE/SPE shall not be used with any other system (Zoom, Microsoft 365, Facebook, LinkedIn, etc.).

POL.IA.L2-3.5.9

Planet Security shall mandate a temporary password, with an immediate change to a permanent password that is consistent with password policy, when administratively resetting an existing user password or when a new user account is created. MFA shall also be mandatory before the authorized account is given access to CUI.

POL.IA.L2-3.5.10

The CPE/SPE shall store and transmit only cryptographically protected passwords.

POL.IA.L2-3.5.11

The CPE/SPE shall obscure feedback of authentication information. CLIENT user shall never use the "Eyeball Feature" when made available.

Incident Response

POL.IR.L2-3.6.1

CLIENT shall establish an operational incident-handling capability for organizational operations that includes preparation, detection, analysis, containment, recovery, and response activities.

Planet Security, Inc. shall incorporate CLIENT system incident-handling capability for the CLIENT CPE/SPE environment that includes preparation, detection, analysis, containment, recovery, and response activities into their existing process.

POL.IR.L2-3.6.2

CLIENT incident response team shall track, document, and report operational incidents to the executive management who will determine if further internal and/or external reporting is necessary and to whom. Initial notification to the executive management shall be within one hour of incident discovery.

The Planet Security, Inc. incident response team shall track, document, and report verified CPE/SPE incidents pertaining to the respective CLIENT organization within 24 hours hour of incident positive verification.

POL.IR.L2-3.6.3

CLIENT shall test the operational incident response capabilities using simulated incident findings at least annually. Results shall be reported to the executive management within a reasonable time frame, not to exceed one week after the conclusion of the testing methodology. Signed copy of the test shall be remitted to Planet Security, Inc. support engineers on the day that it is delivered to the CLIENT executive management so that it may be filed appropriately to support a potential future audit discovery.

Maintenance

POL.MA.L2-3.7.1

Planet Security, Inc. shall exclusively perform maintenance on the CPE/SPE environment.

POL.MA.L2-3.7.2

Planet Security, Inc. shall exclusively control the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

POL.MA.L2-3.7.3

CLIENT executive management shall ensure that equipment that stores, processes, or transmits CUI to be removed for off-site maintenance is sanitized of any CUI prior to its removal from the physical premises. For instance: Prior to a printer being taken off-site for maintenance CLIENT will remove the hard drive. If the printer cannot be repaired, then the hard drive shall be destroyed. Methods of destruction/sanitization shall be consistent with NIST SP800-88.

Planet Security, Inc. will sanitize/destroy the drive at no additional cost to CLIENT if prepaid, mailed/shipped to:

Planet Security Inc.

5325 S Fort Apache Rd. Suite D2

Las Vegas, NV 89148

Please include a note describing the request with an authorized signature. We will contact CLIENT management via Signal Messenger to verify the request.

The drive will not be returned to CLIENT.

POL.MA.L2-3.7.4

The CPE/SPE environment does not allow for CLIENT installation of software.

Operational Technology shall not use physical media for installation of software unless errors, etc. prevent its viable installation. If physical media is used, it shall be scanned for malware before the physical media device is inserted into any device that stores, processes, or transmits CUI.

POL.MA.L2-3.7.5

The CPE/SPE shall use MFA at all times, for all users. Non-local maintenance sessions shall be terminated when maintenance is complete. Maintenance is exclusively performed by Planet Security, Inc.

POL.MA.L2-3.7.6

The CLIENT security team (Often the CCB members as they're already involved with CLIENT security) shall supervise the maintenance activities of maintenance personnel without required access authorization. If the CLIENT team member assigned is not familiar with what the technician is doing, they shall notify the security team lead so that a contextually adept replacement can/will be assigned.

Media Protection

POL.MP.L2-3.8.1

All CLIENT employees and contractors with employee-like access shall protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. CUI assets are to be controlled per procedure: PRO.MP.L2-3.8.1.

POL.MP.L2-3.8.2

CLIENT shall limit access to CUI on system media to authorized users, who shall be assigned based on need-to-know and most restrictive methodologies. System media shall be controlled per procedure: PRO.MP.L2-3.8.2

POL.MP.L2-3.8.3

All media of any kind containing CUI shall be sanitized before disposal or release for reuse. Methods of sanitization shall be consistent with NIST SP800-88r1 or its successor.

For CPE/SPE included media (Backup HDD or USB sticks), please insert the device into an available USB port on the FRONT of the CPE and request that we sanitize it for you via Signal Messenger. We will report back to you when the sanitization is complete.

Write-once media such as CDs etc, must be destroyed as there is no way to sanitize these types of media. Planet Security, Inc. will destroy the media at no additional cost to CLIENT if prepaid, mailed/shipped to:

Planet Security Inc.

5325 S Fort Apache Rd. Suite D2

Las Vegas, NV 89148

Please include a note describing the request with an authorized signature. We will contact CLIENT management via Signal Messenger to verify the request. We will certify the destruction of the media once complete.

POL.MP.L2-3.8.4

The executive management, or designee shall ensure that all media containing CUI is marked indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. CUI marking criteria are defined on this site, under the menu item titled the same.

The term "media" includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking shall not be required for media containing information determined to be in the public domain or to be publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

POL.MP.L2-3.8.5

All CLIENT personnel who are responsible for transporting media containing CUI outside of controlled areas shall be accountable for maintaining the confidentiality of such media. In the event of compromise, notification shall be made to the executive management within 24 hours of discovery who will decide if reporting to the DIBNET is required. If additional assistance is needed, reach out to your Planet Security, Inc. engineering support team via Signal Messenger.

POL.MP.L2-3.8.6

CUI shall be FIPS encrypted to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

POL.MP.L2-3.8.7

Only Planet Security, Inc. supplied removable media shall be used with the CPE/SPE. Both the supplied Hard Drive (Backups) and USB "Flash Drive" provide FIPS validated encryption at all times unless in an unlocked state by the CLIENT.

POL.MP.L2-3.8.8

Only Planet Security, Inc. supplied removable media shall be used with the CPE/SPE. Both the supplied Hard Drive (Backups) and USB "Flash Drive" provide FIPS validated encryption at all times unless in an unlocked state by the CLIENT. You will find these drives MARKED by Planet Security, Inc. for the appropriate usage.

POL.MP.L2-3.8.9

Backup drives for use in the CPE/SPE exclusively use FIPS encryption. These devices are the exclusive method of "Backup". All other methods are prohibited.

Personnel Security

POL.PS.L2-3.9.1

CLIENT shall screen individuals to ensure the person is a US Person prior to authorizing access to CUI.

POL.PS.L2-3.9.2

CLIENT shall ensure that CUI is protected during and after personnel actions such as terminations and transfers. Refer to security procedure: PRO.PS.L2-3.9.2

Physical Security

POL.PE.L1-3.10.1

Physical access to organizational systems, equipment, and the respective operating environments shall be limited to authorized individuals who are assigned using need-to-know and most restrictive methodologies.

POL.PE.L1-3.10.3

All visitors shall be authenticated (US person, who visiting, etc.), properly identified (badged), and always escorted and their activities monitored while beyond the check-in area.

POL.PE.L1-3.10.4

Physical access logs shall be maintained and kept for 3 years. Access to these logs shall be consistent with need-to-know and most-restrictive methodologies. Physical access logs (Scanned or camera phone snapshot with sufficient detail as to be ledgeable) shall be remitted to Planet Security, Inc. by 10am the following workday via Signal Messenger.

POL.PE.L1-3.10.5

Physical access devices (keys, keycards, etc.) shall be controlled and managed based on need-to-know and most restrictive methodologies.

- Number of keys shall be known and documented
- Possession of a key shall be known and documented
    - Person assigned
    - Key number assigned
    - Remaining keys in key lockbox
- Initial key log (Scanned or camera phone snapshot with sufficient detail as to be ledgeable) shall be remitted to Planet Security, Inc. within 30 days of contract signature.

- Updated key logs (Scanned or camera phone snapshot with sufficient detail as to be ledgeable) shall be remitted to Planet Security, Inc. by 10am the following workday after the update via Signal Messenger.

POL.PE.L2-3.10.2

CLIENT approved and assigned personnel shall protect and monitor the physical facility and support infrastructure for the CPE/SPE. Planet Security, Inc. does not currently offer physical security monitoring but if you have questions, we'll help on a "best-effort" basis via Signal Messenger.

POL.PE.L2-3.10.6

Alternative work sites such as telework centers or home-based offices shall maintain the same safeguards as the physical premises. Approved workspaces shall be arranged as to ensure confidentiality of CUI. When leaving the area at any time, CUI shall be logically or physically protected to ensure confidentiality is preserved. Because of privacy concerns, Planet Security, Inc. does not offer (nor do we intend to pursue) alternative worksite security services but if you have questions, we'll help on a "best effort" basis via Signal Messenger.

Risk Assessment

POL.RM.L2-3.11.1

Planet Security will schedule a Zoom call with the CLIENT at approximately the 30 day mark to cover operational security requirements, policies, procedures, and best practices that the CLIENT will need to perform completely to hold up their end of the Statement of Shared Responsibilities.

Planet Security shall come onsite to CLIENT primary location at approximately the 60 day mark from when the contract is signed and assess the operational controls that are required for adherence to the requirements identified in the NIST SP800-171. It is expected that the CLIENT will have implemented all required measures of operational security before this meeting.

Documented findings of non-compliance shall be delivered to CLIENT leadership via Signal Messenger within a week after our visit. The client shall submit documented proof of remediation of the findings within 10 calendar days of receipt of the reporting.

Planet Security shall come onsite (11th month) and annually assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. During this visit, we will pay particular attention to operational security efforts and controls which we do not have visibility from a remote location.

Documented findings of non-compliance shall be delivered to CLIENT leadership via Signal Messenger within a week after our visit. The client shall submit documented proof of remediation of the findings within 10 calendar days of receipt of the reporting.

POL.RM.L2-3.11.2

Planet Security, Inc. shall scan the CPE/SPE environement at least monthly for vulnerabilities monthly on the 15th of each month. In practice (Non-binding), our SIEM tool scans constantly and vulnerabilities are detected within minutes and remediation occurs after COB of the same day of the detection.

POL.RM.L2-3.11.3

When new vulnerabilities affecting systems and applications are identified, remediation shall take place based on the following timetable:

- **Urgent:** Within 24 Hours
- **Critical:** Within 48 Hours
- **High:** Within 1 Week
- **Medium:** Within 1 Month
- **Low:** Within 60 Days
- **Informational:** Remediation not required

Security Assessment

POL.CA.L2-3.12.1

Planet Security, Inc. shall assess the security controls applied to the CPE/SPE to determine if the controls are effective in their application.

Planet Security, Inc. shall assess the security controls applied to the CLIENT operating environment during our annual visit to determine if the operational controls are effective in their application.

POL.CA.L2-3.12.2

Planet Security, Inc. shall develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in the CPE/SPE and at the client operating environment.

POL.CA.L2-3.12.3

Planet Security, Inc. shall monitor the CPE/SPE on an ongoing basis to ensure the continued effectiveness of the required security controls. (NIST SP800-171).

Planet Security, Inc. shall annually assess the CLIENT operating environment to ensure the continued effectiveness of the required operational security controls. (NIST SP800-171).

POL.CA.L2-3.12.4

Planet Security, Inc. shall develop, document, and periodically (Annually or when a significant change occurs) update system security plans for the CPE/SPE environment that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Systems and Communications Protection

POL.SC.L1-3.13.1

The CPE/SPE shall employ automated mechanisms to monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of the CPE/SPE environment. Key internal boundaries shall be defined as an interface that CUI passes from or between a system, host, network, trust-zone or subnet boundary.

POL.SC.L1-3.13.5

The CPE/SPE Network Security Reference Architecture shall provide subnetworks for publicly (RBAC) accessible system components that are physically or logically separated from internal networks.

POL.SC.L2-3.13.2

The CPE/SPE shall employ architectural designs and systems engineering principles that promote effective information security within organizational systems.

POL.SC.L2-3.13.3

The CPE/SPE shall provide and be configured for separate user functionality from system management functionality.

POL.SC.L2-3.13.4

CLIENT shall implement procedures to prevent unauthorized and unintended information transfer via shared system resources (i.e. printers, copiers, etc). Procedure: PRO.SC.L2-3.13.4

POL.SC.L2-3.13.6

The CPE/SPE shall deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

POL.SC.L2-3.13.7

The CPE/SPE environment devices shall not be multi-homed. When used, VPN configurations shall not use split-tunneling.

POL.SC.L2-3.13.8

The CPE/SPE environment shall utilize FIPS validated cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

POL.SC.L2-3.13.9

The CPE/SPE shall employ automated mechanisms to terminate network connections associated with communications sessions at the end of the sessions, or after 120 minutes of inactivity.

POL.SC.L2-3.13.10

The CPE/SPE environment shall employ automated key management mechanisms to establish and manage cryptographic keys for the cryptography schemes employed within the CPE/SPE environment.

CLIENT shall implement the methods from procedure: PRO.SC.L2-3.13.10 for the protection of Keys used to unlock both the HDD (Backup), and USB Flash Drives (Transfer to OT devices).

POL.SC.L2-3.13.11

The CPE/SPE shall exclusively employ FIPS-validated cryptography (140-2 (or) 140-3) when used to protect the confidentiality of CUI.

POL.SC.L2-3.13.12

The CPE/SPE environment shall not allow for remote activation (auto-answer or other similar mechanisms) of collaborative computing devices and provide indication of devices in use to users who are present at the device. Examples of these types of devices are microphones and cameras/webcams. Auto-answer shall be disabled on any such device (i.e. Skype has feature of auto-answer).

POL.SC.L2-3.13.13

Planet Security, Inc. shall monitor the use of Mobile Code within the CPE/SPE environment to detect unauthorized use. Examples of mobile code are javascript, java, flash, OLE, and similar forms of code. Approved formats of mobile code for CLIENT shall exclusively consist of .pdf document generation. All other forms of Mobile Code are prohibited from being produced. (This does not pertain to website flyby whereby the website utilizes javascript or other types of mobile code which are not produced by the CLIENT organization.

POL.SC.L2-3.13.14

Planet Security, Inc. shall monitor the use of Voice over IP technology within the CPE/SPE environment to detect unauthorized use.

Approved uses of VOIP for the CPE/SPE environment shall exclusively consist of teleconferencing and company phone system.

POL.SC.L2-3.13.15

CLIENT shall protect the authenticity of all communications sessions originating from or received by any organizational technologies.

Procedures for this Policy Element: PROPOL.SC.L2-3.13.15

POL.SC.L2-3.13.16

The CPE/SPE shall protect the confidentiality of CUI at rest while within the CPE/SPE environment.

The CLIENT shall protect the confidentiality of CUI at rest while within the CLIENT operational environment.

POL.SC.L2-3.13.17

Under penalty of employee/contract termination and prosecution as authorities may pursue, CUI shall not be published on any external system and/or internal system that is not expressly authorized for the publication of CUI.

Systems and Information Integrity

POL.SI.L1-3.14.1

CPE/SPE security flaws shall be identified, reported, and corrected in a timely manner. Timely is defined in policy element POL.RM.L2-3.11.1

POL.SI.L1-3.14.2

The CPE/SPE environment shall provide protection from malicious code at designated locations within the CPE/SPE environment.

POL.SI.L1-3.14.4

The CPE/SPE shall automatically update malicious code protection mechanisms when new releases are available.

POL.SI.L1-3.14.5

The CPE/SPE shall perform daily scans of all components of the CPE/SPE environment and real-time scans of files from external sources as files are downloaded, opened, or executed.

POL.SI.L2-3.14.3

Planet Security, Inc. shall monitor system security alerts and advisories and utilize the SIEM tool for real-time alerts so that remediation can be accomplished in a timely manner.

POL.SI.L2-3.14.6

The CPE/SPE envonrment shall utilize firewall based intrusion detection systems (IDS) monitor including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

POL.SI.L2-3.14.7

The CPE/SPE environment shall utilize firewall based (IDS) to identify unauthorized use of organizational network based systems. Planet Security, Inc. shall utilze the SIEM to detect unauthorized attempts or usage of Network Operating Systems (RBAC centric)

For questions regarding this Information Security Policy, please reach out to your Planet Security, Inc. Support Engineers using Signal.

Accreditation Statement

On behalf of CLIENT NAME, I hereby issue this Information Security Policy to be effective on the XXth Day of Month, 202X

Chief Executive (Highest Ranking Person Within Client Org)

Date

Statement of Understanding

I attest to the following:

1. I have received a copy of this policy document in either hard or soft form, and have been provided opportunities to ask questions to promote understanding of the Policy.
2. I understand and agree to follow the material within this policy, whether I agree with the material or not.
3. I understand and agree that I shall be held accountable for non-compliance, whether accidental or intentional.

I make this decision to sign of my own free will and am not under duress, or pressure to do so. I understand that my signature is required to gain employment, or contract opportunity, continue the same, and that if I refuse to sign, it will be considered voluntary resignation, contract termination and will not be held against me in the future, with the exception that I understand that if I wish to pursue negotiations at a future time, the same or similar binding policy, subject to updates and applicable laws, shall be required.

____ ________________

Employee or Contractor Signature Date