MSP/Cloud Verify Report – Level 1

Report on Compliance with the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers v.21

As of May 31, 2023

SECTION 1: INTRODUCTION

Dear Reader,

The following service provider has successfully completed the MSP/Cloud Verify Program® (MSPCV). The MSPCV is based on the Unified Certification Standard (UCS) for Cloud and Managed Service Providers® developed by the MSPAlliance®. For 20 years, the MSPAlliance has been promoting the cause of safe and secure outsourcing of IT management to managed service providers. One of the ways MSPAlliance accomplishes this goal is through the UCS.

The UCS consists of 10 control objectives and underlying controls that constitute crucial building blocks of a successful managed services (and cloud computing) organization.

UCS Objective 1: Governance
UCS Objective 2: Policies and Procedures
UCS Objective 3: Confidentiality, Privacy and Service Transparency
UCS Objective 4: Change Management
UCS Objective 5: Service Operations Management
UCS Objective 6: Information Security
UCS Objective 7: Data Management
UCS Objective 8: Physical Security
UCS Objective 9: Billing & Reporting
UCS Objective 10: Corporate Health

During the MSP/Cloud Verify process, the provider is examined by an independent third-party public accounting firm and must demonstrate it has successfully met the applicable 10 control objectives and underlying controls and requirements. The MSPCV examination must be renewed annually.

There are two levels of examination under the MSPCV framework: Level 1, and Level 2.

Level 1 is a "point in time" examination. This means that the service provider met the necessary requirements as of the specified date of its examination.

A first-year Level 2 examination requires a minimum "period of review" of 3 months, while recurring Level 2 examinations typically cover a 12-month period of review. This means the third-party public accounting firm performed sampling and testing in order to verify that the objectives (and controls) were in place and operating effectively during the period of review.

This MSPCV report will describe each control objective, its purpose, and how the service provider has satisfied that control objective. While great care and detail went into the examination of the service provider, in order to protect the security of both the provider and its customers, some details of how the service provider delivers its services, including its security and privacy controls, are discussed here in general terms. By using cloud computing and managed services from a verified provider, you are not only making a wise decision, but you are also helping to ensure that your service provider is abiding by the best practices and standards of a global community of service providers.

Thank you for helping us make the cloud computing and managed services community a safer place. If you have any questions about this examination report you may contact your service provider. You may also request a call with the MSPAlliance and its examination team if you have specific questions about how the examination was conducted.

Signed,

MSPAlliance ®

Chapel Hill, North Carolina

MSPAlliance Est. 2000
International Association of
Cloud and Managed Service Providers

SECTION 2: REPORT BY MANAGEMENT

REPORT BY MANAGEMENT ON THE SERVICES ENVIRONMENT FOR THE MSP/CLOUD VERIFY PROGRAM™ BASED ON THE MSPALLIANCE UNIFIED CERTIFICATION STANDARDS FOR CLOUD AND MANAGED SERVICE PROVIDERS- LEVEL 1

Date

We confirm, to the best of our knowledge and belief, that ProVal Technologies, Inc. maintained effective controls over its Managed Services environment, referred to as its Cloud and Managed Services Environment, throughout the period May 31, 2023. We provide reasonable assurance that ProVal Technologies, Inc. has met, in respect to the MSP/Cloud Verify Program™, based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers v.21- Level 1 requirements of the following objectives:

- Objective 1: Governance
- Objective 2: Policies and Procedures
- Objective 3: Confidentiality, Privacy, and Service Transparency
- Objective 4: Change Management
- Objective 5: Service Operations Management
- Objective 6: Information Security
- Objective 7: Data and Device Management
- Objective 8: Physical Security
- Objective 9: Billing and Reporting
- Objective 10: Corporate Health

The MSPAlliance Unified Certification Standard for, Cloud and Managed Service Providers is available at www.mspalliance.com/ucs. The UCS Objective Summaries and Purposes, along with Management's description of its procedures for compliance therewith, are included in the attached ProVal Technologies, Inc. Description of the Cloud and Managed Services Environment.

DocuSigned by:
Vikram Khanna
DF3F3A057ED8429...

Vikram Khanna, CEO
ProVal Technologies, Inc. Management
07/26/2023

JOHANSON GROUP

SECTION 3: INDEPENDENT ACCOUNTANT'S REPORT

We have examined management of ProVal Technologies, Inc.'s assertion that the requirements in respect to the MSPAlliance Cloud Verify Program based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers for the period of May 31, 2023, is presented in accordance with respect to the MSPAlliance Cloud Verify Program based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers. ProVal Technologies, Inc.'s management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

The information included in Objective 10: Corporate Health provided by ProVal Technologies, Inc. is presented by ProVal Technologies, Inc.'s management to provide additional information on the corporate health of the ProVal Technologies, Inc. While Objective 10: Corporate Health is part of ProVal Technologies, Inc.'s description of its Cloud and Managed Service Environment and the MSPCV Certification Table made available to user entities for the period May 31, 2023, the information about ProVal Technologies, Inc.'s Corporate Health has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

The information included in Section 6: Report Addenda provided by ProVal Technologies, Inc. is presented by ProVal Technologies, Inc.'s management to provide additional information and is not a part of ProVal Technologies, Inc.'s description of its Cloud and Managed Service Environment or the MSPCV Certification Table made available to user entities during the period May 31, 2023. Information about ProVal Technologies, Inc., LLC's SOC 2 Report Addendum, Healthcare Addendum, and ISO Addendum has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Management asserts that ProVal Technologies, Inc. has met the requirements of the MSP/Cloud Verify Program, based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers v.21 - Level 1 including the following objectives:

- Objective 1: Governance,
- Objective 2: Policies and Procedures,
- Objective 3: Confidentiality, Privacy, and Service Transparency
- Objective 4: Change Management,
- Objective 5: Service Operations Management,
- Objective 6: Information Security,
- Objective 7: Data and Device Management,
- Objective 8: Physical Security,
- Objective 9: Billing and Reporting, and

- Objective 10: Corporate Health.

In our opinion, management's assertion that, for the period of May 31, 2023, ProVal Technologies, Inc. has met the requirements in respect to the MSPAlliance Cloud Verify Program in accordance with the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers v.21 - Level 1 is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
July 26, 2023

SECTION 4: DESCRIPTION OF THE CLOUD AND MANAGED SERVICES ENVIRONMENT

ProVal Technologies Inc Background
ProVal Technologies Inc (ProVal Tech) is a Master Managed Service Provider (MSP) based in Orlando, FL, that provides consulting and back-office services to MSP's. ProVal also operates an office in Noida, India. Established in 2008, ProVal Tech serves customers throughout North America.

Services Offered
ProVal Tech provides the following services:

Remote Management and Monitoring (RMM) Consulting: ProVal Tech works with partners to help implement, support, and enhance the RMM tool to meet the MSP's business objectives. ProVal Tech's RMM services include:

- RMM Virtual Admin
- RMM Implementation and Migration
- RMM Training
- Scripting and Automation
- RMM Support and Management

Managed Backup: ProVal Tech monitors and remediates client backup issues 24x7 and provides end-to-end best practice configuration and management of over 30 backup solutions. ProVal Tech's managed backup services include:

- Vendor-agnostic Backup Management
- Initial Setup and Configuration of Backups
- 24x7 Monitoring and Remediation of Backup Failure
- Coordination with Backup Vendors for support
- Daily Error Reporting
- Backup Image and Integrity Verification and Testing
- Backup Platform Migrations

24x7 Network Operation Center (NOC): ProVal Tech provides NOC services for MSPs by proactively monitoring client systems for critical outages and problems. NOC services include:

- Integration with existing tools
- Alert validation
- 24x7 availability
- Initial triage and remediation of critical events
- Escalation of critical issues to the MSPs on-call team
- Ticket updates for all alerts

Services Verified Under MSPCV Report
This MSPCV report has been prepared to provide information on ProVal Tech's compliance with the MSPAlliance Unified Certification Standard v.21. The scope of this MSPCV report is on ProVal Tech's Remote Management and Monitoring (RMM) Consulting, Managed Backup, 24x7 Network Operation Center and in the context of the MSPCV report, Customers are defined as entities utilizing these services.

Events Subsequent to the MSPCV Period of Review
Through its membership in the MSPAlliance, ProVal Tech completed a Service Organization Control (SOC 2 Type 1) Report subsequent to July 1st, 2023. As part of its SOC 2 report, ProVal Tech utilized the UCS objectives and requirements utilized in this report as the basis of the SOC 2 objectives and supporting controls.

External Service Providers Not in Scope of Report
ProVal Tech relies on the encryption controls and the data storage controls (physical security) of their cloud-based applications. Reference to the services provided by these subservice providers is described in the applicable sections of this report. This examination did not extend to the policies and procedures of the subservice providers utilized by ProVal Tech.

Explanation of the MSPCV Certification Table
In the following MSPCV Certification Table, ProVal Tech has disclosed its assertion of compliance with the Objectives and the underlying Requirements of the MSPAlliance Unified Certification Standard (UCS) for Cloud and Managed Service Providers v.21 - Level 1. ProVal Tech's assertion of compliance with the UCS Objectives and underlying Requirements is communicated through the use of the following symbols:

- ✓ - Overall compliance with the UCS Objective has been verified,
- ✓ - ProVal Tech asserts its compliance with the underlying Requirement,
- x - ProVal Tech asserts its compliance with the underlying Requirement is not fully met, or
- * - ProVal Tech asserts its compliance with the underlying Requirement is not applicable to either the services provided by ProVal Tech or is not within the scope of the examination.

As part of the MSPCV process, ProVal Tech is improving their controls and the underlying policies and procedures. While complete compliance with all Requirements is the goal of the examination, no system is perfect. Therefore, non-compliance with a minimal number of Requirements does not prevent overall compliance with the UCS Objective. For instances of noncompliance or a non-applicable Requirement, a summary is provided by ProVal Tech to communicate its mitigation of the root causes for noncompliance.

SECTION 5: MSPCV CERTIFICATION TABLE

UCS Objective 01: Governance

Summary and Purpose *The goal of the Governance Objective is to provide assurance to the Customer that the MSP has established a corporate and organizational structure designed to maximize efficiency, minimize risk, provide sufficient oversight and accountability with regards to the services delivered. This objective also addresses external service provider management protocols of the MSP.*		✓
01.01	**Organizational Structure**	✓
01.02	**Strategic Planning**	✓
01.03	**Risk Assessments**	✓
01.04	**Software Licensing**	*
01.05	**External Service Provider Management**	✓

01.01: Organizational Structure

ProVal Tech uses a team-based organizational structure where the following departments report to the Chief Executive Officer (CEO): Service Delivery, Operations, Finance, Sales & Marketing, and Human Resources. Some departments have teams under them that perform specific functions in the department. An example of this is the Dev Ops team that reports to the Operations department. Each department is led by a department manager, and the CEO meets with each department manager on a weekly basis with recorded notes to track goals set and decisions made during the meetings.

The CEO meets with each department manager on a weekly basis and notes are recorded. The decision-making process is documented and includes the steps of the process.

ProVal Tech does not have a team that has a governing role over the cloud operations, because they do not provide these services.

The internal IT team meets weekly with the Operations Manager and CEO to discuss all decision-making topics. This is formally documented by way of meeting notes each week.

An organizational chart documenting ProVal Tech's operational structure and reporting hierarchy is maintained by Human Resources and made available to all employees.

The ProVal Tech organizational chart is maintained through the organization chart functionality in documentation that renders the chart from Active Directory information, which is updated upon every hire, separation, and organizational change. It is available to all company personnel on their company logins by opening the application. Changes to the organization chart (new hires, separations, and role or reporting changes) are communicated to the workforce through companywide emails.

ProVal Tech has documented job descriptions and requirements for all positions. Requirements such as education and certificates are noted and listed in any job posting. Further, ProVal Tech utilizes a tier progression chart that lines out all requirements for engineers to advance through ProVal Tech’s tier system.

01.02: Strategic Planning
The CEO is responsible for developing the company strategic plans. The strategy is then presented for review and input from the department managers. After the company strategy is finalized, the department managers develop their strategies independently and present them to the CEO and their peers. All strategies must align and support the ProVal Tech short and long-term company strategy.

The strategic plan and priorities for ProVal Tech are updated by the CEO, with input from department managers requested on an annual basis.

01.03: Risk Assessments
ProVal Tech performs an annual risk assessment. Each item is assigned an owner, risk level, and target completion date to help facilitate remediation.

The risk assessment is a living document that is owned by Internal IT and updated based on input from the CEO and ProVal Tech Management.

01.04: Software Licensing
ProVal Tech does not provide Infrastructure as a Service (IaaS) or resell software to Customers.

01.05: External Service Provider Management
External service providers are selected by the CEO using a due diligence spreadsheet to evaluate new external service providers for use in service delivery. A due diligence spreadsheet is completed by Internal IT using various methods on checking references (other MSPs), attending relevant trade shows and user conferences, and internal technical reviews of the vendor before making any selections.

ProVal Tech requests due diligence from all vendors prior to onboarding. The time spent requesting and reviewing vendor due diligence is tracked and documented in a ticket.

ProVal Tech has a documented Vendor Management Policy. The Vendor Management Policy guides the evaluation and assessment of external service providers, allowing ProVal Tech to distinguish external service providers that require additional evaluation and due diligence.

UCS Objective 02: Policies and Procedures

Summary and Purpose *The goal of the Policies and Procedures Objective is to ensure the MSP has documented the necessary policies and procedures in order to maintain effective service delivery levels, as well as to minimize deviation from those established policies and procedures.*		✓
02.01	**Documentation of Policies and Procedures**	✓
02.02	**Data Breach and Cyber-Attack Policies and Procedures**	✓
02.03	**Periodic Review and Approval**	✓
02.04	**Internal Audit**	✓
02.05	**Employee Acceptance**	✓
02.06	**Training and Orientation**	✓

02.01: Documentation of Policies and Procedures
ProVal Tech has documented policies and procedures within their Employee Handbook. This document addresses the following: Company Introduction and CEO's Strategic Vision, Culture, General Administration (Company Property/Travel), Time and Pay Policies, Various Personnel Policies (including overall Code of Conduct) and Recruitment Policies.

The following topics are addressed in the ProVal Tech Information Security Policy: Employee Security, Data Access & Handling, Access Control Policy, and Infrastructure Security.

ProVal Tech utilizes an HR Portal to communicate and monitor adherence to the Employee Handbook and regulatory requirements.

02.02: Data Breach and Cyber-Attack Policies and Procedures
ProVal Tech has a stand-alone policy for Data Breach and Incident Response which applies to all managed and internal systems. This policy addresses ransomware and cyber-attack procedures as well as relevant laws and regulations.

ProVal Tech will formulate a response for Customers that are affected by the data breach and communicate the next steps to the appropriate Customer point of contact.

ProVal Tech stores customer credential information in their documentation system, documentation, contact information in their ticket system, PSA, and billing information in their accounting suite.

ProVal Tech has procedures documented in the Data Breach Policy that cover the company's response and communication of the breach to the appropriate parties. However, it may differ from Customer to Customer; where appropriate, the Customer security officer is notified.

ProVal Tech has not made any ransomware payments within the past 12 months.

02.03: Periodic Review and Approval
ProVal Tech reviews its policies and procedures annually. In the event that changes are made, the new version is published to the employees and the older versions of the document are archived and retained.

ProVal Tech management is responsible for maintenance, administration, and publication of the Employee Handbook and stand-alone policies.

02.04: Internal Audit
ProVal Tech performs an annual internal audit of its controls following a standardized checklist. This audit is tracked in a recurring ticket, and the completed checklist and remediations resulting from the audit are documented in the ticket notes.

The scope and criteria of ProVal Tech's internal audit are documented in the internal audit checklist to guide the performance of the internal audit.

ProVal Tech's leadership is responsible for reviewing and approving the internal audit report upon completion. This approval is documented and dated in the internal audit checklist.

The internal audit results are retained in PSA in recurring tickets.

02.05: Employee Acceptance
Attestation/acknowledgement of the employee handbook is required and is tracked in their HR portals. Employees are required to acknowledge updates to the handbook, which is also tracked in the portal.

Updates to the Employee Handbook or specified policies are communicated to employees via email.

02.06: Training and Orientation
ProVal Tech has a new hire onboarding (orientation/training) program. The framework is documented and can be modified for each position/role. ProVal Tech company and role-specific training are performed for all new hires. Both pieces of training are tracked in a standardized checklist following the new hire training documents.

ProVal Tech has a policy for obtaining outside certifications. These are specific to each role and position and may involve internal or self-study or external training by an external service provider. These are tracked by HR and normally supported by an education application form which allows for the training costs to be paid for by the company.

UCS Objective 03: Confidentiality, Privacy, and Service Transparency

Summary and Purpose *The goal of the Confidentiality, Privacy, and Service Transparency Objective is to ensure the MSP has sufficient policies and procedures related to the protection of Customer data, specifically protocols safeguarding confidentiality, privacy, and geolocation of managed data including external service provider managed data.*		✓
03.01	**Employee Background Check**	✓
03.02	**Employee Confidentiality and Privacy Acceptance**	✓
03.03	**Data Classification and Encryption**	✓
03.04	**MSP Data Geolocation Disclosure**	✓
03.05	**External Service Provider Geolocation Disclosure**	✓
03.06	**External Service Provider Access Management**	*
03.07	**External Service Provider Access Disclosure**	*

03.01: Employee Background Check

ProVal Tech requires background checks for all new employees during the new hire process. The background check verifies SSN and checks national criminal records, sex offender list, address history, county criminal records, and terror watchlist for national, state, and current county of residence. The HR department orders and reviews the checks whenever someone is hired.

03.02: Employee Confidentiality and Privacy Acceptance

ProVal Tech's Employee Handbook contains an internal privacy that states that employees should have no expectation of privacy for files, documents, and assets owned by ProVal Tech. ProVal Tech has all personnel sign the Employee Handbook during the new hire process. All signed forms are stored in ProVal Tech's onboarding software.

03.03: Data Classification and Encryption

ProVal Tech has established a three-tier data classification system, documented in a stand-alone policy, which provides for the following cases: Confidential, Internal/Private, and Public.

ProVal Tech encrypts customer data at rest and in transit using industry best practices. Sensitive client data is contained in either PSA or documentation, both of which are SOC 2 compliant organizations.

03.04: MSP Data Geolocation Disclosure

Customers are informed of the geolocation of their data upon request. This typically occurs prior to onboarding and contract signing if it is a requirement for ProVal Tech’s customer's policies. Data geolocation requests would originate via either the sales process or requested through ProVal Tech consultants. With the request, the disclosure of data geolocation would be handled/responded to by designated ProVal Tech personnel with knowledge of the information.

03.05: External Service Provider Geolocation Disclosure

ProVal Tech does not currently disclose data while in external service provider custody. Customer credential information is stored in documentation servers, contact information is stored in PSA hosted servers, and billing information is stored in billing application hosted

servers. This information has been requested and disclosed in security questionnaires in the past but is not typically requested.

03.06: External Service Provider Access Management
ProVal Tech does not provide external service providers with access to internal or Customer systems.

ProVal Tech does not provide external service providers access to customer data on an as-needed/temporary basis.

03.07: External Service Provider Disclosure
ProVal Tech does not provide continuous or temporary access to third parties.

UCS Objective 04: Change Management

Summary and Purpose *The goal of the Change Management Objective is to ensure the MSP has formalized change management policies and procedures that are under formalized change controls. Such change management documentation may include, if applicable, the capacity planning, modification of MSP and Customer configurations, capacity planning and patch management. Customer change management policies are documented based on the level of services delivered to the Customer by the MSP.*		✓
04.01	**Configuration Documentation**	✓
04.02	**Service Level Categorization**	✓
04.03	**Internal Change Tracking**	✓
04.04	**Customer Change Tracking**	✓
04.05	**Capacity Planning**	*
04.06	**Patch Management**	✓
04.07	**SaaS Special Requirement: Application Development Procedures**	✓
04.09	**SaaS Special Requirement: Development Segregation of Duties**	✓

04.01: Configuration Documentation
Technical and Procedural details specific to the partner, or that deviate from the standard ProVal policy, which is already documented in documentation, are saved in documentation manually by the engineer during the onboarding process.

A standardized PSA Project template is used to ensure consistency. At the start of onboarding, the sales team will set up a kickoff call to introduce the engineer. Client communication is consistent throughout the process to ensure expectations are properly set with progress.

Once a Customer notifies ProVal Tech of their desire to add services, the Account Management Team is responsible for initiating and completing the contractual changes. The contractual changes are processed through the updating of the original agreement. Once the contractual changes have been completed by the Account Management Team, a ticket is created to onboard the services. Any change to services requires formal approval by the designated Customer contact. This approval is recorded via a contract addendum if it requires a contract change. If the service is already covered by the existing contract, then the request can be made and approved via a ticket.

Once a Customer notifies ProVal Tech of their desire to remove services, the Account Management Team is responsible for initiating and completing the contractual changes. The contractual changes are processed through the approval of the termination of service notice. Once the contractual changes have been completed by the Account Management Team, a ticket is created to offboard the service.

04.02: Service Level Categorization
ProVal Tech uses PSA to classify and identify all new, existing, and former Customers. Companies are identified by Name and Agreement Types. Every active Customer has an agreement corresponding to the product or service to which they subscribe. All companies with

an active Managed Service Agreement are given a status of active in PSA. This allows Service Delivery to process requests for these Customers. ProVal Tech has two SLAs for ticket priorities that drive different response and resolution goals by priority. Low, Medium, and High priority tickets follow the Standard SLA, and Critical Priority tickets follow the Critical SLA. These priorities apply to all Customers. ProVal Tech does not offer different priority or SLAs by Customer

04.03: Internal Change Tracking
ProVal tracks internal changes in PSA. ProVal has a documented Change Management Policy that outlines rules to be followed in the change management process. Employees can submit a request for a change as an internal change ticket, which is tracked in the internal IT ticket board. Once submitted, the change is reviewed during the morning Internal IT meeting, where an employee documents the approval or rejection of the change. The implementation of the change is tracked in a new ticket or project, depending on the size and scope of the change.

04.04: Customer Change Tracking
ProVal's clients are themselves MSPs. Any request for change by the MSP's client(s) has/have been expressly approved prior to the request reaching ProVal. ProVal does not guarantee change tracking for client environments in any contract. All changes made by ProVal are, however, documented thoroughly in the relevant ticket / project task.

04.05: Capacity Planning
ProVal Tech asserts its compliance with the underlying Requirement is not applicable to either the services provided by ProVal Tech or is not within the scope of the examination.

04.06: Patch Management
ProVal Tech has a documented Patch Management Policy that defines a recurring set of patching procedures. ProVal Tech performs patching and remediation via RMM and the Patch Management interface. ProVal Tech utilizes an automated patch approval process within RMM to release critical patches internally. The patch approval process is supplemented by patch recommendations from a patch verification subscription service.

ProVal Tech applies patches one week after their release to circumvent a vendor recall and relies on the vendor to perform all necessary testing of patches before release. If the patch wasn't recalled in the following week and ProVal Tech does not receive notice of issues, patches are selected and applied during the Customer's maintenance window.

As ProVal Tech manages MSPs as a whole, they do not have specific maintenance windows unless specified by the client. If the client specifies a maintenance window, it is recorded in documentation and referenced by the team.

04.07: SaaS Special Requirement: Application Development Procedures
Software development lifecycle and release management procedures have been documented to define the process for requesting, logging, approval, testing, and acceptance of changes to the ProVal Tech environments.

The company handles application changes through a change request and source control model. All change requests are approved by the Development Team Lead, assigned for work, and completed if approved. Testing is undergone to ensure proper operation of the content, and then the changes are tracked in a centralized location available to all relevant team members.

04.09: SaaS Special Requirement: Development Segregation of Duties

The Client's RMM is the production environment in this case. ProVal Tech develops content based on client request, provides the content once complete, and the client then decides whether to release this content to their endpoints. Content developed by ProVal is fully reviewed and tested and is only implemented in the client environment with explicit approval by the client.

UCS Objective 05: Service Operations Management

Summary and Purpose

The goal of the Service Operations Management Objective deals with how the MSP identifies and responds to IT related events that could impact services delivered to the Customer. In this UCS objective, the examination covers the MSP's Network Operations Center ("NOC"), Trouble Ticketing systems and Service Desk operations specifically related to event management policies and procedures.

✓

05.01	**Centralized Operations Center**	✓
05.02	**Support and Problem Logging**	✓
05.03	**Categorization and Correlation**	✓
05.04	**Support and Problem Resolution**	✓
05.05	**Operations Monitoring**	✓

05.01: Centralized Operations Center

ProVal Tech has a mobile staff that operates from a virtual NOC. The ProVal Tech VNOC is staffed by engineers who monitor and manage the devices under contract on a 24x7 basis. The majority of the staff assists Customers during normal business hours with multi-threaded coverage overnight and during weekend hours and holidays.

ProVal Tech operates a 24/7 Virtual Network Operations Center. The schedule is made based on team member availability and is published to Teams for members.

05.02: Support and Problem Logging

Customer support issues are handled through the ticketing system. Issues may be called into the dispatcher who then creates the ticket or emailed directly to the ticket system from the Customer. All new tickets are triaged by the dispatcher and assigned metadata that includes the contract agreement, type, and subtype of the issue for categorization. Priority may be assigned based on the number of people affected and the business impact on the Customer.

NOC alerts are created from the monitoring systems and automatically create tickets in the ticketing system. The interface for the ticket creation is dependent on the monitoring system and includes a two-way API and inbound email connector. Non-critical NOC tickets are dispatched by the dispatcher to the engineers.

The RMM has the capability to self-remediate certain types of alerts via automation scripts. Alert tickets may be automatically closed by the monitoring application if the alert condition no longer exists. Tickets that are created by Customers or other users only automatically close if a client response is not received in a timely manner (48 hours). Logged tickets are never deleted and maintained for reporting and historical reference within the ticketing system.

Contractual SLAs are defined within the ticketing system based on the agreement defined within the ticketing system. The agreement is based on the signed contract/Work Order with the Customer. The SLA for response time is then automatically tracked by the ticketing system based on status changes for each ticket. SLA status is available on a dashboard within the ticketing system on the Service board screen. Additionally, reports are built into the ticketing system that can be run on demand.

05.03: Categorization and Correlation
API and email connectors are utilized to automatically categorize tickets; email, portal, and phone call tickets have manually set priorities and categorization. Documentation is maintained on each ticket referencing the primary ticket in which the event is handled.

Correlation of tickets is a manual operation where the staff can merge related cases into a master ticket, grouped by Customer based on alerts. The merge is manually processed by the MSP personnel and is utilized to ensure that tickets are adequately addressed.

05.04: Support and Problem Resolution
Ticket documentation requirements are defined in Incident Ticket Creation Policy. Ticket documentation and categorization standards are to be adhered to for all tickets on relevant PSA dashboards.

ProVal Tech's ticketing system is configured to automatically send ticket update and closure emails to customers.

ProVal Tech's policy is that all Customer support issues/request communication be logged in the corresponding support ticket. Any Customer communication regarding events identified in monitored environments should be logged in the corresponding ticket. Special considerations for Customer monitored environments (typically co-managed environments) are documented in PSA.

05.05: Operations Monitoring
ProVal Technologies Management shall conduct internal reviews of tickets and operational events on a quarterly basis. The review process is documented in the policy and includes review of resolved and unresolved tickets, KPI indicators, effectiveness of collaboration, and tool usage.

UCS Objective 06: Information Security

Summary and Purpose *The goal of the Information Security Objective is to ensure the MSP has implemented necessary controls to effectively govern access to managed data, networks and systems that may compromise security of both the MSP and the Customer. This includes remote access policies, user account administration, authentication, wireless access, segregation of duties, network security scans and assessments, and the monitoring of access to Customer systems.*		✓
06.01	**Access to Applications and Environments**	✓
06.02	**Super User and Administrator Access Security**	✓
06.03	**Unique Users and Passwords**	✓
06.04	**Revocation of Access**	✓
06.05	**Strong Passwords**	✓
06.06	**Segregation of Access**	✓
06.07	**Periodic Review of Access Rights**	✓
06.08	**Secure Remote Access**	✓
06.09	**Network and Endpoint Security Management and Monitoring**	✓
06.10	**Email Security**	✓
06.11	**Antivirus**	✓
06.12	**Wireless Network Security**	✓
06.13	**Network Security Assessments**	✓

06.01: Access to Applications and Environments

ProVal Tech has outlined within the Information Security Program document to confirm personnel has network access based on defined roles and responsibilities by job role and ProVal Tech's security group naming convention matches job roles for easy access. Access to ProVal Tech's internal applications is also granted by job role. Customer system and data access are restricted to ProVal Tech's technical personnel.

Local workstation and communication tools are secured with AD with MFA enforced. Remote access to client environments is done through a remote desktop, which is configured to use SSO against AD identity services. Internal applications, such as the antivirus portal, RMM, and documentation are secured with MFA. ProVal Tech's PSA is secured with SSO against AD identity services. Any applications that are not compatible with SSO and/or MFA are configured with secured local accounts.

Access provisioning follows ProVal Tech's set process. The Human Resources department submits a form that creates a ticket that includes the department, manager, and department of the employee. Internal IT creates an initial employee account and routes the ticket to other system owners for access to systems that Internal IT may not administer.

When a user's role is changing in the company, Human Resources submits a form that creates a ticket to track the change. Internal IT receives the ticket, grants new accesses and removes old access, and documents the ticket.

06.02: Super User and Administrator Access Security
ProVal Tech follows a Role-Based Access Control policy as stated in the ProVal Tech Information Security Policy. Administrative rights are restricted to accounts only accessible to ProVal Tech Internal IT team and upper management. Furthermore, domain Global Administrator accounts are split from daily use accounts. Changes to administrative roles for any internal applications are tracked through a change process logged through PSA tickets.

Default passwords for any application or device are changed to meet ProVal Tech's password policy during provisioning. When the application allows, passwords are set to require a reset on first login. Passwords are documented company wide. Documentation is centrally managed by Internal IT, with access to the passwords being restricted to authorized ProVal Tech personnel in a role that requires access.

06.03: Unique Users and Passwords
ProVal Tech Employees do authenticate to the company network using unique username and passwords. ProVal Tech follows a first.last name naming convention for network accounts and applications that support first.last naming. If multiple employees have the same first and last name, ProVal Tech will use middle initials to uniquely identify personnel.

ProVal Tech utilizes AD authentication for all applications that allow this type of authentication. This in turn allows ProVal Tech personnel to use their ProVal Tech network username and password so they're uniquely identified by name. In the event an application does not support AD authentication, ProVal Tech will utilize the first and last names as a naming convention to uniquely identify accounts. Application access and the security level are based upon role/job function. ProVal Tech also utilizes SSO/MFA for VPN access to client networks.

ProVal Tech does not utilize guest accounts or grant guest access to ProVal Tech's own network.

In compliance-sensitive Customer environments, service personnel utilize a user-unique administrator credential for support and administration functions. For non-compliance-sensitive Customer environments, service personnel are permitted to use a shared administrator credential that is stored in documentation. All remote access and functions are automatically logged and tracked to the individual user via ProVal Tech's use of RMM, PSA, and documentation. Access to passwords within documentation is tracked as part of that service offering.

06.04: Revocation of Access
All employee terminations are processed in the same manner whether they're involuntary or voluntary and all access (network, application, and physical) is revoked immediately upon completion of the HR exit interview. Terminations are tracked in a PSA Ticket on the Internal IT Service Board. These tickets have an associated template with a specific set of instructions that details the steps for ProVal Tech internal team to process the termination.

06.05: Strong Passwords
ProVal Tech has a documented password policy with the Information Security Program policy document. ProVal Tech's password policy requires unique passwords with a minimum of eight characters and must contain a combination of upper- and lower-case letters, numbers, punctuation and other special characters. Additionally, AD has a lockout policy configured to lock accounts for a minimum of one minute after ten unsuccessful login attempts. Applications

that support inherent authentication are enforced to the extent possible by the applications. The password policy also requires that all company passwords, including credentials to customer environments, be stored and encrypted in ProVal Tech's documentation instance.

ProVal Tech enforces its password policy by requiring all passwords to be stored in documentation Enterprise. This ensures that all company passwords meet ProVal Tech's requirements.

06.06: Segregation of Access

ProVal Tech has logical segregation of access based on role/job function. These roles are translated to security groups that restrict access to shared folders/documents based on membership. Application access is granted by employee role as well. For example, no Service Delivery personnel at ProVal Tech have access to Accounting/Billing, and ProVal Tech Finance/HR personnel do not have access to applications such as remote desktop, customer networks, infrastructure, or any customer environment credential information. Additionally, NOC access to customer environment information is further restricted to only support personnel who are assigned to that customer.

Employees are only given access to applications required for their role. Additionally, access is further segregated in the application through the use of defined roles, when applicable.

ProVal Tech has an Access Control Policy that contains a high-level explanation of the company's access segregation methodology. Additionally, ProVal Tech has a logical security matrix that outlines which types of employees are allowed to access which applications within the company.

06.07: Periodic Review of Access Rights

Changes to ProVal Tech employee roles, employee offboarding and employee offboarding are audited monthly through an Internal IT recurring RMM ticket. Upon receiving the ticket, Internal IT requests a list of changes to employee roles and status from the HR department. Internal IT then verifies, for each item, that onboarding accounts were provisioned correctly in Active Directory and application-level accesses. For offboarding accounts, Internal IT verifies that the account has been removed or converted to a shared mailbox when applicable, as well as verifying that the user's accounts have been deactivated in ProVal Tech applications. For role changes, Internal IT verifies that the new accesses were successfully changed and that old accesses have been revoked.

06.08: Secure Remote Access

ProVal Tech utilizes Control for remote access to Customer environments. Further, Control uses LDAP/AD integration, MFA Authentication, and it is restricted for use by Service Delivery personnel. All Customer remote sessions are logged via remote desktop and stored for 90 days. A remote session report is available upon Customer request and delivered monthly. Remote access to the company's network is only permitted with work-issued equipment and the company's VPN is also secured by Multi Factor Authentication.

Reviews are completed only when an event has been identified by either internal resources or Customers. If the review is requested by a Customer, the review request and performance would be documented within a ticket.

06.09: Network and Endpoint Security Management and Monitoring

ProVal Tech has implemented antivirus on their endpoints to scan and block traffic of malicious origin or destination. These events generate alerts, and when they cross a predefined threshold will send an email that generates a ticket in the Internal IT service board for triage, investigation, and remediation when applicable.

ProVal Tech infrastructure utilizes network segmentation to isolate applications at the network level. Network firewalls are implemented at every segment of the network, with rules to only allow authorized traffic. ProVal Tech employs separate network firewalls at the datacenter level for bare metal and cloud servers. Office locations are secured with network firewalls. Endpoints utilize Windows Firewall to block traffic from home networks. VPN access is provided which authenticates users through SSO with MFA enforced and provides encrypted network access to endpoints defined in an ACL. Web content filtering provided by antivirus is in place for all endpoints.

ProVal Tech maintains copies of the security configurations for all firewalls. These copies are stored in ProVal Tech's company documentation application and can be referenced in the event the security configurations need to be rebuilt. The copies are updated when changes are made, and older versions of the documents are retained for archives.

Internal Firewall events are logged and incidents requiring intervention or review are emailed to ProVal Tech's PSA and placed on the Internal IT board for review, for internal infrastructure. For client-facing infrastructure, External service provider has full control and monitoring capability over the network edge.

ProVal Tech does not provide firewall management and monitoring as a service.

ProVal Tech does not provide SIEM as a service.

06.10: Email Security

ProVal Tech utilizes Microsoft 365 Exchange Online Protection to secure internal email. The email security solution includes spam filtering, email encryption, attachment scanning, data loss prevention, and business continuity. Additionally, NOC and support personnel are restricted from being able to send and receive emails outside of the organization. Alerts generated from Exchange Online are sent to the PSA Internal IT service board for triage.

ProVal Tech does not offer or provide email protection or scanning services to Customers.

06.11: Antivirus

ProVal Tech employs antivirus and antimalware solutions to secure assets internally. The antivirus product is integrated with RMM and is focused on file scanning for signatures and is always active. This antivirus also includes a DNS filter that blocks name resolution to known bad URL's/DNS names. Antivirus is managed via a centralized dashboard to provide visibility to all protected endpoints, with alerts from the solutions logged on the Internal IT Service Board in PSA for Internal IT personnel to triage and investigate.

ProVal Tech does not offer or provide Antivirus services for customers.

06.12: Wireless Network Security

ProVal Tech has implemented access points to secure and manage wireless access points at the main office and branches which are password protected.

ProVal Tech's office does not allow guests and does not provide a guest Wi-Fi network.

06.13: Network Security Assessments
Full port scans are conducted against all external IP addresses on a bi-annual basis. The results of the scans are logged in a recurring PSA ticket, and a formal report is attached to the ticket and sent to designated upper management for review/approval.

The results of the scan are reviewed by the Owner, CTO, and vCIO. The review is documented in a service ticket.

ProVal Tech does not maintain or operate a traditional corporate LAN nor do they host infrastructure on a LAN. Network scans are conducted against the public IP addresses of our cloud and hosted infrastructure.

UCS Objective 07: Data and Device Management

Summary and Purpose *The goal of the Data Management Objective is to confirm the MSP has sufficient policies and procedures to ensure the integrity and availability of managed Customer and MSP internal data in the event of natural disasters, cyber-attacks (i.e., ransomware), and user error or malfeasance. This includes the implementation of data backup as well as encryption, security, retention, and restoration of managed Customer and MSP internal data.*		✓
07.01	**Customer Data Backup and Replication**	✓
07.02	**MSP Data Backup and Replication**	✓
07.03	**Data Recovery Testing**	✓
07.04	**Disaster and Business Continuity Planning**	✓
07.05	**Internal Data Destruction**	✓
07.06	**Customer Data Destruction**	*
07.07	**Device and Asset Management**	✓

07.01: Customer Data Backup and Replication
ProVal Tech maintains data backup policy within documentation. PoVal monitors backup jobs through automated tickets that are generated on the Backups or service board in PSA. The standard retentions are set by the MSP and are monitored by ProVal and set during onboarding. ProVal Tech maintains a shared Note document that contains customer specific backup requirements and procedures.

Encrypted at rest and mechanism depends on the solution the client MSP is using. Some clients additionally opt to encrypt data in transit as well. Backup/recovery implements AES256 encryption. In the event of an issue with the backup, the ProVal Tech team is notified through a ticket to the Backups or ProNoc PSA service boards.

ProVal Tech does not manage the MSA with the MSP's customers. ProVal tech works off the MSA with the MSPs and not work with the MSPs clients. Customer encryption requirements are documented in the MSP's backup SOW. This SOW is followed when configuring the MSP's and the MSP's end client's backups.

07.02: MSP Data Backup and Replication
ProVal Tech backs up its internal data using a combination of cloud provided instance backups and offsite backups for self-hosted applications. Offsite backups are encrypted and stored in cloud storage. The status of the offsite backups is reported and reviewed daily.

ProVal Tech has a documented Data Backup and Retention Policy that defines encryption requirements for internal backups. Offsite backups of self-hosted applications are required to be encrypted at rest and in transit.

07.03: Data Recovery Testing
Backup data restoration and recovery testing procedures are conducted for backup Customers on a quarterly basis. The initiation and results of the testing procedures are scheduled and documented in a ticket in the Customer's PSA. Internal backups are tested on an annual basis and are tasked and tracked through a ticket.

07.04: Disaster and Business Continuity Planning
ProVal Tech has a Business Continuity Plan that is tested annually. The results of the test are documented in a PSA ticket.

07.05: Internal Data Destruction
ProVal Tech has a documented Data Destruction Policy that outlines the steps and rules for their internal data destruction. Laptop hard drives are removed prior to recycling, zeroed, and stored in a locked cabinet in the office locations. ProVal Tech utilizes multiple vendors that perform secure and observed data destruction when the drives are determined to be end of life.

07.06: Customer Data Destruction
ProVal Tech does not offer data destruction services to Customers.

07.07: Device and Asset Management
ProVal Tech has a documented Device Policy that includes the definition of devices and contains requirements for the management of mobile and personal devices to mitigate the risks associated with mobile and personally owned devices.

ProVal Tech maintains an inventory list of assets in an excel spreadsheet. Assets are added and removed from this spreadsheet during periodic review of the list.

UCS Objective 08: Physical Security

Summary and Purpose

The goal of the Physical Security Objective is to ensure the MSP has documented policies and procedures governing physical access and environmental security of the MSP's assets. MSP must demonstrate sufficient physical security controls at each facility, including controls such as physical access administration, card key, CCTV, on-site security, visitor/guest logs and other effective security and environmental controls.

✓

08.01	**Office Security**	✓
08.02	**Logging of Visitors**	✓
08.03	**Sensitive Area Security**	*
08.04	**Revocation of Physical Access**	✓

08.01: Office Security

ProVal Tech is a mostly remote organization that has two office locations for employees to meet face to face once a week. ProVal Tech offices are locked and secured at all times. However, due to the nature of the services provided, ProVal Tech personnel and services are rendered remotely and follow a Virtual Clean Desk Policy that applies to all employees.

Physical access to the ProVal Tech offices is not critical to the delivery or security of Managed Services. The ProVal Tech offices do not contain any infrastructure or datacenters, and there are no VPN tunnels connecting the offices together or to ProVal Tech cloud infrastructure. ProVal Tech offices also do not contain any restricted or sensitive areas. No sensitive information is contained in the offices and eliminates the risk to ProVal Tech Customers.

ProVal Tech asserts its compliance with the underlying Requirement is not applicable to either the services provided by ProVal Tech or is not within the scope of the examination. ProVal does not conduct Physical Security Assessments.

08.02: Logging of Visitors

Visitors to ProVal Tech must sign the visitor's log sheet that is maintained close to the Main Entrance of all offices. The log must show the date, name of the visitor, visitor's signature, identification used, purpose of the visit, time in/out, and the name of the authorized escort.

08.03: Sensitive Area Security

ProVal Tech asserts its compliance with the underlying Requirement is not applicable to either the services provided by ProVal Tech or is not within the scope of the examination. ProVal tech does not have sensitive areas (including operations centers, data centers, and server rooms) in ProVal Tech's office locations.

08.04: Revocation of Physical Access

When an employee leaves ProVal Tech, physical termination procedures are defined in a Human Resources process document that is saved in the HR file sharing platform. During the procedure, HR opens a ticket with Internal IT to revoke access. Access revocation occurs when the employee is notified of the termination. Revocation of access to the VPN and SSO terminates access to all Customers and services. If the employee was issued a physical key to the office, it is also revoked.

UCS Objective 09: Billing and Reporting

Summary and Purpose *The goal of the Billing and Reporting Objective is to ensure the MSP is accurately monitoring service delivery, reporting, and invoicing for Customers in accordance with SLAs signed by both parties.*		✓
09.01	**Signed Contracts and Agreements**	✓
09.02	**Accuracy of Service Invoices**	✓
09.03	**Report Availability**	✓

09.01: Signed Contracts and Agreements
ProVal Technologies has written agreements between ProVal Tech and their clients that outline Scope of Work, Pricing, Client requirements, and SLAs. The contract is signed by the client, the CEO, and the document preparer, who will either be the Sales Manager or Operations Manager.

09.02: Accuracy of Service Invoices
ProVal Tech's Customers are invoiced for services rendered by ProVal Tech's following the service defined in the signed contracts. Time spent by IT Support Personnel to support Customers outside of the terms of contracts is recorded and entered into the billing system for invoicing. Invoicing is performed by the Controller, with invoices being reviewed for adherence to the terms of the contract by an Account Executive and ProVal Tech Partners before issuance.

09.03: Report Availability
Reports are provided to customers via monthly administrative calls between the account manager and the client. Notes for this call are documented. ProVal Tech does not have a contractual requirement in any SoW for reporting.

UCS Objective 10: Corporate Health

Summary and Purpose *The goal of the Corporate Health Objective is to ensure sufficient corporate and financial health on the part of the MSP so that all of its Customers are adequately protected. Technical proficiency is only part of the MSP's value to the Customer. The MSP must be on firm financial footing, as well as risk averse in a variety of areas unique to managed services and cloud in order to effectively deliver its services to the Customer.*		✓
10.01	**Operational Sustainability**	✓
10.02	**Significant Customer Risk**	✓
10.03	**Gross Profit Margin of Services**	✓
10.04	**Customer Commitments**	✓
10.05	**Insurance**	✓
10.06	**Customer and Employee Retention Tracking**	✓

10.01: Operational Sustainability
ProVal Tech was incorporated/formed in 2008 and has been providing services to Customers for over 13 years. As of the date of this report, ProVal Tech's financials showed that its operations were profitable over the previous 12 months. This profitability indicates operational sustainability and fiscal responsibility.

10.02: Significant Customer Risk
ProVal's top five Customers represent approximately 5% of total ProVal revenue, which is less than the UCS best practice of 50% from the top five Customers. The largest ProVal Customer represents only 3% of total ProVal revenue which is less than the UCS best practice of one Customer not representing more than 20% of total revenue. Due to this, ProVal is considered to have minimal risk due to a loss of a significant Customer.

10.03: Gross Profit Margin on Services
ProVal maintains a gross profit margin on its services, which exceeds the UCS best practice of 30%. By exceeding the best practice, it shows that ProVal is operationally efficient in its costs of delivering services.

10.04: Customer Commitments
The majority of contracts have a term of 3 months. ProVal utilizes month-to-month contracts on a limited basis, with those contracts supporting specific services or service lines.

10.05: Insurance
ProVal Tech carries insurance coverage commensurate with UCS best practices, including cybersecurity, errors and omissions, and professional liability.

10.06: Customer and Employee Retention Tracking
Over the last fiscal year, ProVal has a managed services Customer retention rate of approximately 90% and an employee retention rate of 95%.

SECTION 6: SOC 2 ADDENDUM

SOC 2 Report Addendum

Unified Certification Standard→ MSPAlliance® for Cloud and Managed Service Providers

FOR PROVAL'S SOC 2 MAPPING

This MSP/Cloud Verify Program™ (MSPCV) report for ProVal Technologies Inc (ProVal Tech) is based on the control objectives of the Unified Certification Standard for Cloud and Managed Service Providers (MSPs) (UCS) v.21. The UCS establishes best practices for MSPs in the delivery of their services to customers. The UCS generally applies to most MSPs around the world, regardless of their vertical or market expertise and focus.

A Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) is a report that describes how a Service Organization meets the criteria defined in a set of Trust Services Criteria (TSCs)[1].

The following table represents the mapping of the ProVal Tech MSPCV report to their SOC 2 report[2]. This table was included in the issued and unqualified 2023 ProVal Tech SOC 2 Type 1 report on Security, Availability, and Confidentiality.

Trust Services for the Security, Availability, and Confidentiality Principles	**MSPAlliance UCS Objectives**									
	01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**
CC 1.0 Common Criteria Related to Control Environments										
CC 1.1 The entity demonstrates a commitment to integrity and ethical values.	✓	✓	✓		✓					
CC 1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	✓									
CC 1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	✓									
CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	✓	✓	✓							
CC 1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	✓	✓								

[1] TSC section 100, *Trust Service Criteria for Security, Availability, and Confidentiality, 2017* (AICPA, *Trust Services Criteria*)

[2] The TSC does not address the requirements of UCS Objective 9: Billing and Reporting and UCS Objective 10: Corporate Health.

CC 2.0 Common Criteria Related to Communications and Information

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		✓	✓	✓	✓					
CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	✓	✓	✓	✓	✓		✓	✓		
CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	✓		✓	✓				✓		

CC 3.0 Common Criteria Related to Risk Management

CC 3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	✓		✓	✓						
CC 3.2 The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	✓		✓							
CC 3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.	✓		✓	✓	✓					
CC 3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.	✓									

CC 4.0 Common Criteria Related to Monitoring Activities

CC 4.1 The entity selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	✓			✓						
CC 4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	✓	✓		✓		✓				

CC 5.0 Common Criteria Related to Control Activities

CC 5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			✓	✓						
CC 5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.		✓	✓	✓						
CC 5.3 The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.		✓		✓						

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information	✓		✓	✓		✓	✓			

assets to protect them from security events to meet the entity's objectives.										
CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.						✓		✓		
CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.						✓				
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.								✓		
CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.							✓			
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.				✓		✓		✓		
CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.				✓		✓	✓			
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.				✓		✓	✓			

CC 7.0 Common Criteria Related to System Operations

CC 7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.				✓	✓	✓				
CC 7.2 The entity 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; anomalies are analyzed to determine whether they represent security events.		✓			✓		✓			

CC 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		✓			✓	✓	✓			
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		✓			✓					
CC 7.5 The entity identifies, develops and implements activities to recover from identified security incidents.					✓					
CC 8.0 Common Criteria Related to Change Management										
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.				✓		✓				
CC 9.0 Common Criteria Related to Risk Mitigation										
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	✓	✓		✓						
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	✓		✓							
A 1.0 Additional Criteria for Availability										
A 1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.				✓				✓		
A 1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.							✓			
A 1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.							✓			
C 1.0 Additional Criteria for Confidentiality										
C 1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		✓	✓				✓			
C 1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			✓				✓			

COMPANY INFORMATION

Examined Company:

ProVal Tech
498 Palm Springs Drive, Ste. 310
Altamonte Springs, FL 32701
Phone: (407) 588-0101
https://www.provaltech.com

Independent 3rd Party Auditor:

Johanson Group, LLP
6547 N Academy Blvd, Colorado Springs, Colorado, 80918, United States
Phone: (719) 434-0750
https://www.johansonllp.com/

Examining Body:

MSPAlliance®
Phone: 800-672-9205
www.mspalliance.com