Category	Classification	#	Item	Determination	Conformity Status	Notes
Access Control	Basic Security Requirements	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	○	Access to each system is limited to the minimum number of authorized operational users. Access by RPA is also limited to only the range of users on behalf of said users.	Microsoft365 admin rights: representative employee User administrator only granted to Secretary. Other organizational administrator rights for remote desktop environment, domain services, and website management (Wordpress) have also been granted to the Representative Employee only.
		3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	○	Guest and anonymous accounts are not created and are operationally prohibited from being created. For shared accounts (company representative email accounts), access is restricted to representative employees and Secretaries only. Test accounts for development can be created only with prior permission from the system administrator. For each personal Windows environment, remote access is allowed but data transfer to the client side is denied.	
	Derivative Security Requirements	3.1.3	Control the flow of CUI in accordance with approved authorizations.	△	(1) Information whose export is restricted should not be transferred across the Internet using plaintext. →The network is encrypted and does not enable movement in plain text. (2) Blocking traffic from outside that is claimed to be from within the organization. →Network access from outside is denied. (3) Blocking requests to the Internet that do not come from internal web proxy servers →The business environment is limited to terminals managed by our VDI server or MDM, and access is permitted only from the designated server. (4) Limiting information transfer between organizations based on data structure and content. →Information transfer between organizations is physically separated and limited.	The network environment is managed by the office management company and all details, including specifications, are not available. It has been tested and confirmed that there is no external access to the office network environment. Access between tenants in the office has not been confirmed.
		3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	△	(1) Assigning mission-related functions and system support-related functions to different individuals or roles →Both are authorized by the representative employee. (2) Different individuals perform system support functions (e.g., configuration management, quality assurance and testing, system administration, programming, and network security). →If the representative employee performs the function, it is implemented by more than one person, for example, the Secretary performs the review. (3) Ensuring that security personnel who manage the access control function do not also manage the audit function → Audit process not yet implemented.	
		3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	○	Privileged accounts are granted to the minimum required. (Currently, only the representative employee holds such privileges.) Set up in such a way that local accounts cannot be created (client management privileges are managed by the representative employee, and users can only use accounts with assigned user privileges).	Client user permissions do not allow for additional users or programs
		3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	×	Administrative privileges are the same as those of the representative employee account, and non-privileged accounts are not available.	Microsoft365、TeamViewer
		3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	○	Non-privileged users are prevented from executing privileged functions. The implementation history is recorded in the OS log.	
		3.1.8	Limit unsuccessful logon attempts.	○	The number of failed logon attempts is limited, and the account is locked after a predetermined number of incorrect attempts.	
		3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	○	For company-loaned smartphones, the company labels them as company-owned and controlled.	
		3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	○	The system is set to go into a screen lock state when inactive for a certain period of time. In addition, the system usage rules restrict the screen lock to be applied when the user leaves his/her seat.	
		3.1.11	Terminate (automatically) a user session after a defined condition.	○	Remote desktop sessions to each individual's Windows environment are set to disconnect when the client side enters sleep mode.	
		3.1.12	Monitor and control remote access sessions.	○	Account usage during remote access can be monitored and connection logs are recorded. The VDI environment can also be monitored on the server side in real time for usage status.	
		3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	○	At the remote access tool, the session is encrypted (encryption is based on 4096-bit RSA private/public key exchange and 256-bit AES session encoding).	https://community.teamviewer.com/Japanese/kb/articles/4619-teamviewer%E3%81%AE%E5%AE%89%E5%85%A8%E6%80%A7%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6
		3.1.14	Route remote access via managed access control points.	○	Remote access is allowed only from designated tools, not from unmanaged access control points. The network environment in the office is basically inaccessible from the outside.	
		3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	○	All servers and clients (except mobile devices) can be accessed remotely.	
		3.1.16	Authorize wireless access prior to allowing such connections.	○	Connection to wireless access is restricted by password. Some locations also restrict connections by the device's Mac address.	
		3.1.17	Protect wireless access using authentication and encryption.	○	Wireless access is password-authenticated (in some cases, Mac address authentication is also used) and encrypted.	
		3.1.18	Control connection of mobile devices.	○	Mobile devices can only access the work environment from devices that have been registered with MDM in advance. When accessing the work environment from a personally-owned mobile device, the device is automatically registered with MDM and the connection can be managed.	
		3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	○	Mobile devices are encrypted.	
		3.1.20	Verify and control/limit connections to and use of external systems.	○	The use of Saas verifies authentication with IDs and passwords. The administrator registers the IDs and passwords that can be used to connect in advance, limiting the number of accounts that can use the system.	
		3.1.21	Limit use of organizational portable storage devices on external systems.	○	The company does not own any portable devices. The use of personally-owned portable devices is prohibited by the company's usage rules.	
		3.1.22	Control CUI posted or processed on publicly accessible systems.	○	The rules of use do not allow information to be posted in publicly accessible locations. Information posted on the official Web site is checked by a representative employee.	
Awareness and Training	Basic Security Requirements	3.2.1	Ensure that managers, systems administrators, and users of organizational systems 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.	○	Each member of the company is informed of the security policy by the representative employee. The contents related to the security policy (rules) are posted on the company's portal site and made known to all employees.	
		3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	○	Each member is educated on security matters related to the performance of his/her duties using educational materials.	
	Derivative Security Requirements	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	○	The company's service regulations prohibit matters that pose an insider threat, and rules prohibit individual employees from handling such matters. Representative employees are encouraged to exchange information and raise awareness through frequent communication.	
Audit and Accountability	Basic Security Requirements	3.3.1	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.	○	Access to business systems is monitored and logged.	
		3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	○	E-mail and chat history is maintained on an individual basis and is uniquely traced.	
	Derivative Security Requirements	3.3.3	Review and update logged events.	○	Log events are reviewed as needed.	
		3.3.4	Alert in the event of an audit logging process failure.	×	Alerts for audit logging process failures are not being issued.	
		3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	×	There is no review and analysis of audit records in operation.	
		3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	○	The tools are equipped with functions to support the analysis.	Microsoft365、TeamViewer
		3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	△	The logs are time-stamped, but the time zone varies between logs.	
		3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	○	The audit log does not possess a basic deletion function. Even if a privileged account can delete them, deletion is not operated. In addition, privileged accounts are limited to the representative employee only.	
		3.3.9	Limit management of audit logging functionality to a subset of privileged users.	○	Limited to the representative employee only.	
Configuration Management	Basic Security Requirements	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	×	Not documented.	
		3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems	×	There is no documentation of security configuration settings.	
	Derivative Security Requirements	3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	×	The process for approving or disapproving changes is not defined. In addition, changes cannot be tracked.	
		3.4.4	Analyze the security impact of changes prior to implementation.	△	The security impact is analyzed through a simple assessment by the system administrator.	
		3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	△	The company stipulates that only the representative employee has access to the system, but this is not documented.	
		3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	○	Only the minimum required functions and services are provided. The scope of provision is reviewed by the system administrator from time to time.	
		3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	△	Some functions used only for system administration (command prompt, registry editor, etc.) are also available.	
		3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	○	Policies are applied and whitelisted.	
		3.4.9	Control and monitor user-installed software.	○	Software installed by users is managed and monitored by a dedicated management tool.	
Identification and Authentication	Basic Security Requirements	3.5.1	Identify system users, processes acting on behalf of users, and devices.	○	Each account is unique, and the user is also identified by the device. In addition, the company's representative account is shared only with the representative employee and the Secretary, but the user can be identified by the IP address from which he/she logged in.	

		3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems	○	Individual accounts are two-step authenticated by using a password as well as a dedicated authenticator-application.	
	Derivative Security Requirements	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	○	Access by privileged and non-privileged accounts is two-step authenticated by a dedicated authenticator-application.	
		3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	○	The process is designed to allow the response to replay operationally.	
		3.5.5	Prevent reuse of identifiers for a defined period.	○	IDs and other information are made unique to prevent reuse.	
		3.5.6	Disable identifiers after a defined period of inactivity.	○	IDs are inventoried as needed and unnecessary IDs are disabled.	
		3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	○	Password policies enforce minimum complexity and character changes.	
		3.5.8	Prohibit password reuse for a specified number of generations.	×	It has not been prohibited.	
		3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	○	Temporary passwords are set to be compulsorily changed at the first login.	
		3.5.10	Store and transmit only cryptographically-protected passwords.	○	Passwords are encrypted.	
		3.5.11	Obscure feedback of authentication information.	○	Passwords are displayed as asterisks.	
Incident Response	Basic Security Requirements	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	△	Incident handling training has not been conducted.	
		3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	×	Incident reporting process is not documented.	
	Derivative Security Requirements	3.6.3	Test the organizational incident response capability	×	Tests have not been conducted.	
Maintenance	Basic Security Requirements	3.7.1	Perform maintenance on organizational systems.	○	The system is maintained as needed.	
		3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	○	Maintenance is managed by a single substitute employee.	
	Derivative Security Requirements	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	○	All information is stored in the cloud, so basically no information is stored locally. In addition, off-site maintenance is generally not performed.	
		3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	○	The system is constantly checked with tools that detect malicious code.	TeamViewer Malwarebytes
		3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	○	Currently, sessions are not established during maintenance.	
		3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	○	Currently, maintenance is performed only by the representative employee who is the system administrator.	
Media Protection	Basic Security Requirements	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	×	Paper and digital (NAS) are not stored in locked cabinets.	
		3.8.2	Limit access to CUI on system media to authorized users.	×	Physical access is not restricted.	
		3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	○	System media is physically destroyed when discarding. When reused, they are sanitized.	
	Derivative Security Requirements	3.8.4	Mark media with necessary CUI markings and distribution limitations.	○	Currently no target media.	
		3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	○	Currently no target media.	
		3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	○	Digital media are encrypted.	
		3.8.7	Control the use of removable media on system components.	×	The use of removable media is not controlled.	
		3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	○	Operational rules prohibit the use of portable storage devices.	
		3.8.9	Protect the confidentiality of backup CUI at storage locations.	○	Backup data is encrypted.	
Personnel Security	Basic Security Requirements	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	○	Access to the system is reviewed by the system administrator.	
		3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	○	All loaned devices are returned upon resignation and are protected by changing account passwords.	
Physical Protection	Basic Security Requirements	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	○	The server location is locked and keys are given only to authorized individuals. Access to the satellite offices is also limited to the representative employee and the Secretary.	
		3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	○	The office is monitored using video surveillance equipment. In addition, the opening and closing of locks is logged.	
	Derivative Security Requirements	3.10.3	Escort visitors and monitor visitor activity.	○	Visitors are accompanied and monitored by a team member at all times.	
		3.10.4	Maintain audit logs of physical access.	○	The video surveillance system's motion detection feature automatically records the video. Door unlocking is also logged with an account and date/time log.	
		3.10.5	Control and manage physical access devices.	○	It is supervised by a combination of locks and a smart lock system.	
		3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	○	The company has established rules for conducting duties when working remotely.	
Risk Assessment	Basic Security Requirements	3.11.1	Periodically 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.	×	Regular assessments are not being conducted.	
	Derivative Security Requirements	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	○	Vulnerability scans are performed at all times. Detected vulnerabilities are addressed at least once a week.	
		3.11.3	Remediate vulnerabilities in accordance with risk assessments.	○	Vulnerabilities are removed according to the 3.11.2 scan.	
Security Assessment	Basic Security Requirements	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	×	Regular assessments are not performed.	
		3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	×	The implementation plan has not been prepared.	
		3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	○	The system administrator continuously monitors the system.	
		3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	×	The plan has not been prepared.	
System and Communications Protection	Basic Security Requirements	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	×	A system capable of monitoring the contents of communications is not yet established.	
		3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	△	Layered protection is being developed.	
		3.13.3	Separate user functionality from system management functionality.	○	User functions can be physically or virtually separated.	
		3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	○	Although the only shared system resource is the company representative account, the usage environment is virtually separated to prevent unintended information transfer.	
		3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	×	Sub-networks have not been implemented.	
		3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	○	Network communication traffic is allowed or denied by the firewall.	
		3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	○	The user is set up in a way that does not allow for any configuration changes.	
		3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	○	All communication content is encrypted.	
		3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	○	When accessing remotely, the session is set to automatically disconnect as soon as the specified inactivity time has passed, as well as to lock the screen.	
		3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	×	The requirements have not been defined.	
		3..13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	○	FIPS-certified encryption technology is used.	
		3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	○	There are no co-computing devices.	
		3.13.13	Control and monitor the use of mobile code.	○	The system administrator reviews, controls and monitors usage on a case-by-case basis.	
		3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	○	The system administrator reviews, controls and monitors usage on a case-by-case basis.	
		3.13.15	Protect the authenticity of communications sessions.	○	Remote access tools protect authenticity through the tool's functionality.	
		3.13.16	Protect the confidentiality of CUI at rest.	×	No protection during communication outage.	
System and Information Integrity	Basic Security Requirements	3.14.1	Identify, report, and correct system flaws in a timely manner.	○	Identified and revised as needed.	
		3.14.2	Provide protection from malicious code at designated locations within organizational systems.	○	Protection is provided by EDR.	
		3.14.3	Monitor system security alerts and advisories and take action in response.	○	A tool is being implemented to issue security alerts for the system.	
	Derivative Security Requirements	3.14.4	Update malicious code protection mechanisms when new releases are available.	○	The system is set to update automatically when released.	
		3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	○	It is performed regularly and on a case-by-case basis.	
		3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	×	System monitoring is not in place.	
		3.14.7	Identify unauthorized use of organizational systems.	×	System usage is monitored but not at the traffic level, nor can it be identified.	