Ⅰ.Basic information

	◆Basic topic		
1	Governing Law for the Services.	According to Japan	
2	Applicable Data Protection Law for the Service	Personal Information Protection Act	
3	The posession of the data registered in the service.	Service user	
4	Have you established policies regarding information security and personal information protection, and have you publicized these policies both inside and outside the organization?	○	
5	Have they obtained third-party certification for information security or personal information protection?	○	・Privacy Mark: Updated August 19, 2022 ・ISMS（ISO/IEC 27001）：Updated March 23, 2022
6	Are there any relevant laws, regulations, and contractual requirements that service providers and cloud services must meet, and are there ongoing efforts to meet these?	○	
7	Are security measures regularly evaluated by an external auditing department to see whether they are implemented correctly and operating as intended, and whether they comply with relevant laws, regulations, and contractual requirements?	○	We conduct external audits.

Ⅱ.Items related to personal information protection

	◆Privacy Policy and Data Use		
8	Has the personal information protection policy been disclosed to service users?	○	
9	If laws and regulations related to personal information protection apply, will you be able to comply with those requests?	○	
10	Does the service collect personal information?	○	
11	Does your company use personal information of service subscribers?	○	This information is anonymized and used for marketing purposes.
12	Are personal information of service subscribers provided to third parties?	×	
13	Does your company use the data entrusted to it by service subscribers?	○	
14	Do you provide the entrusted data of service subscribers to third parties?	×	
15	Will the deposited data be transferred to other countries through the use of external services or outsourcing?	×	
	◆Disclaimer		
16	Are there any service levels defined?	○	We have SLA Refer：https://h-t.co.th/assets/pdf/sla_en.pdf
17	Does it specify conditions, such as disclaimers of liability, for use of the service?	○	This is stipulated in KING OF TIME article 12 Refer：https://h-t.co.th/assets/pdf/term-of-use.pdf

Ⅲ.General Security

	◆Information Security		
18	Have you specified a person responsible for information security management and defined his/her job scope, authority and responsibilities?	○	
19	Regarding information security, have roles and responsibilities been defined not only for normal times but also for emergency situations?	○	
20	Have the relevant departments, duties, and functions regarding information security management been clarified?	○	
21	Are you properly dividing up what you will handle in-house and what you will outsource, and clearly defining roles and responsibilities?	○	
22	In order to reduce the risk of unauthorized or unintended changes or misuse, are authorities for accessing, viewing, modifying, etc. information assets separated according to organizational roles and responsibilities?	○	
23	In order to raise awareness of information security and the handling of important information, we regularly provide appropriate education and training, and we continue to provide education in any areas where understanding is lacking.	○	
	◆Security measures for employees		
24	Are employees provided with education and training to prepare for security incidents?	○	
25	Do you have confidentiality agreements in place with your employees?	○	
26	When contracts with employees and contracting parties are terminated or changed, are access rights changed or deleted, loaned assets returned, etc.?	○	
	◆Information Asset Management		
27	Have you established a management process and criteria for importance of information assets, identified and evaluated information assets in accordance with the management process, and created a list of assets?	○	
28	When erasing information assets or disposing of components such as servers or media, is the data written therein rendered unrecoverable?	○	Storage media has been physically destroyed.
29	Do contracts, terms, etc. clearly state how data will be handled when service usage ends?	○	When you cancel your contract, we will immediately erase your data logically. However, we will not delete it from the backup data and will encrypt it.
30	When the service usage ends, can the data entrusted by the service user or the data created by the service user be returned and deleted?	○	There are no refunds, but they are being removed.
	◆Access Restrictions		
31	Have procedures been established for the storage, movement, disposal, and scope of users of external storage media, and are media used in accordance with these procedures?	×	It is not stored on external storage media.
32	Have you established and implemented an access control policy for the software, hardware, and data handled on the network used in the development, maintenance, and operation of cloud services?	○	
33	Are employees and system administrators in principle prohibited from accessing deposited data from service users? When access to deposited data is necessary for business purposes, is it limited to those who have been approved in advance, and are operation logs of those accessing the data monitored?	○	Logging in to your environment is only possible with your permission.
34	Is access to components and data within cloud services restricted to only employees who have a business need for each component?	○	

35	Are network access to information assets using privileged accounts recorded and monitored for appropriate use?	○	
36	For cloud services, are any unnecessary accounts or accounts that have not been used for a certain period of time (including accounts due to transfer, retirement, or role change) disabled or deleted?	○	
37	In principle, the use of shared accounts is prohibited, and even if their use is approved as an exception, is appropriate use confirmed through management records, usage logs, etc. (The confirmation method should be described in the remarks column.)	○	
38	Is the system designed so that an issued ID cannot be issued to another person in duplicate?	○	
39	Are you restricting connection routes based on source IP addresses?	○	It is possible to restrict the IP address from which connections are made by changing your settings.
40	Are there any appropriate authentication mechanisms in place, such as multi-factor authentication, single sign-on, or two-step authentication?	○	
41	Are accounts that fail authentication a specified number of times consecutively locked or prevented from authenticating for a certain period of time?	○	
42	Is communication encrypted when sending and receiving authentication information?	○	
43	If no operation is performed within a certain period of time after logging in, does the session end and require the user to log in again?	○	The expiration time is set to 30 minutes.
44	Regarding passwords, are they case-sensitive, contain a combination of letters, numbers and special characters, and have a minimum character length to ensure the necessary complexity?	○	
45	Is the password you enter not displayed on the screen?	○	
46	Are passwords stored and transmitted only encrypted?	○	
47	Have you set minimum and maximum password lifetimes?	○	
48	Do you prohibit the reuse of the same password across generations?	○	
49	Are default passwords being used on cloud service servers and components?	○	
50	Is it possible for users to change their own passwords?	○	
51	When assigning and using privileged accounts in the development, maintenance, and operation of cloud services, is approval required and is it limited to the bare minimum?	○	
52	Are you restricting access to administrative privileges and privileged utilities for cloud services and applications?	○	
53	Are those who have access to program sources and specifications, etc., restricted?	○	
54	Do you control the access in place to limit who can release or launch changes to your cloud services?	○	
◆Encryption of data and communications			
55	In order to protect information assets, has an encryption policy been established according to importance and use?	○	
56	Are encryption keys and passwords controlled so that they can be accessed only by limited system administrators when necessary?	○	
57	Is data stored in the service encrypted or masked so that the contents of the data cannot be recognized when the database or file is accessed directly?	○	
58	Are access controls for the database and access logs monitored?	○	
59	Is the backup data encrypted so that the contents cannot be recognized?	○	
60	Are access controls and access logs for backup data being monitored?	○	
61	If SSL communication is used, is communication using vulnerable communication protocols prohibited?	×	Some of our time-stamping machines use TLS 1.0 and 1.1, but we plan to prohibit them in the future.
62	Is communication encrypted when accessing a website?	○	
63	Are you using an unexpired SSL server certificate issued by a trusted certificate authority?	○	We use an SSL server certificate issued by GlobalSign.
◆Physical and Environmental Security			
64	Are physical security perimeters defined to protect certain areas of data and data processing facilities based on the criticality of the assets within the perimeter?	○	
65	Is entry to security areas permitted based on approval, and is entry controlled by authentication such as IC card authentication or biometric authentication?	○	
66	Are entry and exit logs regularly checked to ensure there is no unauthorized access?	○	
67	Are measures being taken, such as installing surveillance cameras in particularly important locations and having a witness accompany ?	○	
68	Are you using an in-country region and data center?	○	
69	Are you using international regions and data centers?	○	
◆Security Regarding Service Operation			
70	Have the functions, component structure, specifications, conditions of service provision, usage methods, etc., of the cloud service been documented?	○	
71	Are cloud service changes reviewed, and are system and network configurations visualized to confirm there are no unauthorized changes?	○	
72	Are the functions and operations of cloud services regularly reviewed, and are any deficiencies addressed?	○	
73	Are the impacts of changes to cloud services clearly documented and visualized?	○	
74	Are only approved changes provided in the cloud service?	○	
75	Are the identified defects and their management in the cloud service reported according to the prescribed methods?	○	
76	Are there established rules for providing prior notice of major service changes or termination to service users?	○	
77	Are the hours for providing services set and notified to service users?	○	Notification via login screen and email
78	Are notification rules for immediate or additional information set and implemented in case of service disruptions or performance degradation in the cloud service?	○	Notification via login screen and email
79	Are rules for prior notification to service users established for emergency or irregular maintenance related to the cloud service provision?	○	Notification via login screen and email
80	Are the handling of entrusted data specified in terms, agreements, and personal data protection policies, and disclosed to the service contractors?	○	

81	Is management performed to meet system requirements or address resource shortages caused by denial-of-service attacks?	○	
82	Is resource management conducted with consideration for future needs, not only current status?	○	
83	Are tests performed in a development environment equivalent to the production environment in advance to resolve issues and prevent defects caused by changes to the production environment?	○	
84	Is malware protection software actively deployed, along with regular updates to pattern files, for the cloud service and all its essential components, including the terminals used for service delivery?	○	
85	Is the cloud service's time managed uniformly across all components (time zone) and synchronized using mechanisms such as NTP?	○	
86	Is software installation and modification work restricted to authorized devices using device authentication, MAC address authentication, and source IP address restrictions?	○	
◆About Backup			
87	Are the cloud service and data backed up to enable recovery within predetermined target times?	○	
88	Are restore tests conducted to ensure proper recovery from backups for the cloud service?	○	
89	Is it confirmed that backups of the cloud service have been taken?	○	The system backs up data until 4:00 AM on the previous day.
90	Are the cloud service backup data stored in a physically separate location (different region) from the location where the cloud service is deployed?	○	
◆About Log Acquisition			
91	Are event and access logs being collected to record errors related to system failures, exception handling, incorrect operations, and security incidents?	○	
92	Are logs of login and logout events for service users and system administrators being recorded?	○	
93	Are operational logs for service users and system administrators being recorded?	○	
94	Are data retention periods and management requirements for data and logs defined and implemented in accordance with relevant laws and regulations?	○	
95	Is there a system in place to efficiently analyze cloud service logs for immediate analysis of incidents following a security event?	○	
96	Are access controls and encryption being applied to protect collected logs and backup data from unauthorized access and tampering?	○	
◆About Vulnerabilities			
97	Are vulnerability assessments being conducted for cloud services?	○	We perform simple diagnostics weekly, including port scans, detailed network diagnostics, and penetration tests.
98	When changes are made to cloud service infrastructure, network, or operations, are functional, non-functional, and security vulnerability assessments conducted to ensure that no impacts or issues arise after these changes?	○	
99	Are vulnerability assessments carried out prior to any changes in cloud services, and are measures taken based on the results of these assessments?	○	Vulnerability assessments—including those for web applications, networks, and mobile applications—performed by specialized inspection agencies before the service launch, following public releases after corrections or changes, and at least once a year.
100	Is information regarding vulnerabilities and End of Service Life (EOSL) for operating systems, middleware, and software regularly collected, and are patches or software updates applied as necessary?	○	
101	Is there a policy in place for addressing vulnerabilities according to their risk levels and timelines, and are vulnerabilities managed in accordance with this policy?	○	
◆About Security Incident			
102	Are there established procedures to handle security incidents and system failures?	○	
103	Is performance monitoring conducted on cloud services and networks to detect security incidents and system failures?	○	
104	Is there monitoring in place for service uptime, failures, and external operational monitoring to detect security incidents and system failures?	○	
105	Is monitoring conducted to detect unauthorized access and misuse, both internally and externally, regarding security incidents and system failures?	○	
106	Is there monitoring in place for suspicious network packets to detect security incidents and system failures?	○	
107	Is monitoring conducted for unauthorized network access and remote access to detect security incidents and system failures?	○	
108	Are roles and responsibilities clearly defined to ensure swift and effective responses to security incidents and system failures?	○	
109	Are recovery plans and emergency response plans established to prepare for disasters, such as earthquakes, fires, or major system failures?	○	
110	Is the scope of security incidents and the notification procedures for users clearly defined?	○	In the event of a leak, loss, or damage to customers' personal information, notifications will be issued immediately via email and posted on the company's website, including relevant details. Furthermore, the results of the investigation will be promptly communicated through email and shared on the company's website once the investigation is completed.
◆About Network Security			
111	Is prior approval from a system administrator necessary to access cloud services remotely?	○	
112	Is a firewall installed to prevent unauthorized access from both external and internal sources?	○	
113	Are pattern files and definitions for unauthorized access prevention devices regularly updated?	○	
114	Is a WAF implemented to protect against attacks that exploit web application vulnerabilities? ※ WAF …Web Application Firewall	○	
115	Are the pattern files and definitions for the WAF regularly updated? ※ WAF … Web Application Firewall	○	
116	Are measures in place to counter attacks that may disrupt service maintenance and operation, such as DDoS? ※ DDoS … Distributed Denial of Service attack	○	

117	Are pattern files and definitions regularly updated to protect against disruptions in service operation?	○	
118	Is there a process in place to promptly notify system administrators and service users of any detected unauthorized access?	○	
119	Can the service-using company restrict access to cloud services based on the IP address of the connection source?	○	
120	For accessing the management screen used for the development, maintenance, and operation of cloud services, can access routes be restricted based on the IP address of the connection source?	○	
121	In cloud services, are boundaries protected by logical separation according to the function of each server?	○	
122	Are database (DB) servers separated from web servers, with access controls that limit communication routes between the web server and the DB server to the minimum necessary?	○	
123	Are access controls implemented to prevent direct access to the database (DB) server from external sources?	○	
124	In the exchange of information within cloud services, are encryption and check digits utilized in transmission paths to ensure the confidentiality and integrity of information?	○	
◆About the Development and Maintainance of Cloud Service Systems			
125	Are security requirement specifications clearly defined in the development, maintenance, and operation of cloud services?	○	
126	In every stage of cloud service development, maintenance, and operation, are functional requirements, non-functional requirements, and security requirements identified and reviewed to ensure security and quality?	○	
127	In every stage of cloud service development, maintenance, and operation, are secure coding practices and security test reviews conducted to ensure security and quality?	○	
128	In every stage of cloud service development, maintenance, and operation, are approval processes and data modification processes established to ensure security and quality?	○	
129	In the development, maintenance, and operation of cloud services, is there a separation between development and production environments to prevent data leaks?	○	
130	In the development, maintenance, and operation of cloud services, is duplication or external use of data from the production environment (such as for testing) prohibited to prevent data leaks?	○	
131	Are restrictions and monitoring in place to ensure that prohibited software is not used on terminals involved in cloud service development, maintenance, and operation?	○	
132	When changes are made to applications, are tests conducted in advance to confirm that there are no impacts or issues post-change?	○	
◆About Management of External Contractors			
133	Do external contractors use entrusted data?	○	Only to be used when necessary, such as for support tasks, bug investigations, and similar activities.
134	Are external contractors required to meet information security standards equivalent to our company's?	○	
135	Are external contractors evaluated on a regular basis?	○	The evaluations conducted at least once a year.