Information Disclosure Guidelines for Safety and Reliability of ASP / SaaS

*1 For “Essential” items of disclosure, if presence or absence is asked, answer is “present” or “absent”.

*2 If one of “Essential” items is not disclosed, certification is not given.

*3 Among “Essential” items, especially important items are marked as “O”, and certification is assumed to be given if all these items can meet certain requirements.

*4 Name of representative is essential. Information of other items is optional.

Business enterprise	Items for Information Disclosure	Description (*1)	Definition etc.	Essential (*2)/ Optional	Items which should consider specific requirement (*3)	
Time of the Information Disclosure	Date of the Information Disclosure	Year, month, date of information disclosure		Essential		
Place of business enterprise / Business						
Business Enterprise Overview	Name of business enterprise	Formal name of business enterprise (trade name)		Essential		
	Established Year / Years in Business	Established year of business enterprise, number of years in business		Essential		
	Office (enterprise place)	Place of head office of business enterprise, number of offices(domestic and foreign), locations of major offices		Essential		
Business overview	Principal business overview	Overview of principal business of business enterprise in addition to ASP / SaaS business		Essential		
Human resources						
Management	Representatives	Name of representative Picture, age, background of representative (academic, career, certificate etc.)		Essential (*4)		
	Executives	Number of executives, names of executives		Optional		
Employees	Number of employees	Number of regular employees		Optional		
Financial Conditions						
Financial Data	Sales	Sales of entire business enterprise in the most recent financial year (consolidated base)		Essential		
	Ordinary profit	Ordinary profit of the entire business enterprise in the most recent financial year (consolidated base)		Optional		
	Capital	Capital of the entire business enterprise in the most recent financial year (consolidated base)		Essential		
	Equity ratio	Ratio of equity capital of the entire business enterprise in the most recent financial year (consolidated base)	○Equity ratio =[Equity capital] / [Total assets]	Optional		

	Debt to Cash Flow ratio	Interest bearing debt to cash flow ratio of the entire business enterprise in the most recent financial year (consolidated base)	○Debt to Cash Flow ratio =[Interest bearing debt] / [Operating cash flow]	Optional		
	Interest coverage ratio	Interest coverage ratio of the entire business enterprise in the most recent financial year (consolidated base)	○Interest coverage ratio =[Operating cash flow] / [Interest payment]	Optional		
Financial Reliability	Listing on stock markets	Whether or not business enterprise is listed on stock market, name of market if listed		Optional		
	Situation on Financial audit / Financial data	Select appropriate situation from the following; accounting audit by accounting auditor, audit by accounting adviser, financial data based on checklist according to small and mid-sized enterprise accounting, or none of the above.		Optional		
	Mandatory publication of financial statements	Whether or not financial statement is published mandatorily		Optional		
Capital relationship / Business connections						
Capital relationship	Shareholder composition	Names of large shareholders (largest 5) and ratio of stock holding of each shareholder		Optional		
Business connections	Major trading partners	Names of major trading partners		Optional		
	Main dealing financial institution	Name of main dealing financial institution		Optional		
	Member organization	Name of industry organizations, economic organizations and others which enterprise belongs		Optional		
Compliance						
Organization-system	Executive for Compliance	Name of executive for compliance		Optional		
	Full-time section and meeting committee structure	Presence or absence of full-time section and meeting committee structure which is responsible for compliance, name of section and meeting committee if present		Optional		
Rulemaking and documentation of rules	Policies on the information security	Presence or absence of basic policies, organizational rules, manuals etc, on the information security Names of documents if present, and whether or not they are approved by managements (Although the contents of documents are not disclosed, submission is required as examination documents for certification)		Essential	O	Certification is not given if documents such as information security rules are absent

	Policies on the invitation and sales	Presence or absence of basic policies, organizational rules, manuals etc. on the invitation and sales Names of documents if present, and whether or not they are approved by managements (Although the contents of documents are not disclosed, submission is required as examination documents for certification)		Optional		
	Policies on the complaint procedure relating to ASP / SaaS	Presence or absence of basic policies, organizational rules, manuals etc. on the complaint response procedure relating to ASP / SaaS service Names of documents if present, and whether or not they are approved by managements (Although the contents of documents are not disclosed, submission is required as examination documents for certification)		Essential		
Service	**Items for Information Disclosure**	**Description (*1)**	**Definition etc.**	**Essential (*2)/ Optional**	**Items which should consider specific requirement (*3)**	
Basic features of services						
Content of services	Name of services	Name of ASP/SaaS service applied		Essential		
	Start date of services	Year, month, date of service launch of ASP/SaaS service applied (If major renewal has occurred between service launch and application, state year, month, date of the renewal)		Essential		
	Basic types of services	Select appropriate type from the following; application service, network platform service, ASP platform service, or other service		Essential		
	Contents and scope of services	Content and characteristics of ASP/SaaS service applied Description of service collaboration with other business enterprise if present		Essential		
	Limitation on service customization	Range of application customization (It not defined or to be discussed separately, describe so)		Essential		
Change / termination of services	Prior notice of the change or termination of services	Time and method of notification to users (Describe time of prior notice using such units as 1 month prior, 3 months, 6 months, and 12 months)		Essential	O	Certification is not given if user notification time is less than 1 month prior

	Response and alternative measures for the change or termination of services	Presence or absence of basic policies on response and alternative measures, outline if basic policies are present Presence or absence of response to users at contract termination (introducing alternative service etc.), outline of response if present Presence or absence of responsibility to return information assets (user data etc.) at contact termination		Essential		
	References relating to the change or termination of services	Presence or absence of point of contact (including one for regular complaints), name and opening hours of point of contact if present		Essential	O	Certification is not given if point of contact is not present
Prices for the services / Cancellation	Charging methods	Charging methods of measured rate portion and fixed rate portion respectively		Essential		
	Pricing structure / Prices	Amount of initial cost, monthly charge, minimum contract duration		Essential		
	Penalty for cancellation of the contract	Presence or absence of cancellation penalty (which user must pay), amount of penalty fee if present		Essential		
	Term for the prior notice of cancellation from users	Presence or absence of term for the prior notice of cancellation from users, due date if present (describe how many days/months prior the notice should be made)		Essential		
Quality of Service	service availability ratio	Actual value of service availability If actual value cannot be described by an unavoidable reason, the reason and target value must be described Pattern number of type of service in "Information Security Guideline" and counter measured reference value History of service suspension accidents	○Service provision time =[contract service time] – [service suspension time announced in advance for regular maintenance] ○Service availability ratio = [actual service available duration] / [service provision time]	Essential	O	Certification is not given if service availability ratio does not reach certain level (required figures will be determined for each application based on discussion results of "ASP/SaaS information security Committee")
	Management of service performance	Method of detection of equipment failure and system delay (point of detection, detection interval , detection method such as screen display check) Method to understand service performance (point of detection, detection interval , detection method such as screen display check)		Optional		
	Reinforcement of service performance	Presence or absence of system reinforcement determination criteria or plan Outline technical measures (load balancing , network routing, compression etc.) if determination criteria or plan is present		Optional		

	Acquirement of Certification / Implementation of Audits	Acquirement of Privacy mark, ISMS, ITSMS, presence or absence of audit report created upon ASCR18 (SAS70 in US) Name of certification or audit if the above is present		Optional		
	Treatment of personal information	Clear indication of purposes of collecting personal information		Essential		
	Vulnerability assessment	Target of assessment (application, OS, hardware etc.) Frequency and response to assessment result, state of countermeasure taken for required portion (for each target)		Optional		
	Interval on verifications of backup data integrity	Backup execution interval Generations of backup data(describe the number of generations)		Essential		
	Maintenance for backup data	Interval of verification of backup data		Essential		
	History of award or commendation	History of awards received relevant to ASP/SaaS service		Optional		
	Service level agreement (SLA)	Whether or not SLA relevant to this certification items is attached to contract		Essential		
Amount of services used	Number of users	Number or user licenses for ASP/SaaS service applied (identify if this is the number of concurrent users or actual users)		Optional		
	Number of agencies	Number of agency of ASP/SaaS service applied		Optional		
Application, Infrastructure, Storage						
Contents	Core software	Name and overview of core application		Essential		
	Name of provider of the core software	Name of enterprise that provides core application		Essential		
Cooperation / Scalability	Method of cooperation with other system	Use of standard API with which cooperation is available, name of API if standard one is used, availability of disclosing API if non-standard one is used		Optional		
Security	Live-or-death monitoring (software, equipment)	Presence or absence of live-or-death monitoring, monitoring target if live-or-death monitoring is carried out (application, platform, storage etc.), and monitoring interval, monitoring time, notification time of each live-or-death monitoring target	○Monitoring interval: Duration in minutes at which monitoring is carried out (time interval) ○Monitoring time =[Actual monitoring time] / [Service provision time] ○ Notification time: Time before live-or-death monitoring result is notified to designated administrator	Essential	O	Certification is not given if live-or-death monitoring is not available
	Fault monitoring (software, equipment)	Presence or absence of fault monitoring		Essential		

	Time Synchronization	Method of time synchronization of system		Essential		
	Anti-virus measures	Presence or absence of antivirus measure, if present, update interval of pattern file (time from vendor release)		Essential	O	Certification is not given if antivirus measure is not taken
	Record (Log)	Usage of users, whether or not record of exception handling and security event (log etc.) is taken, how long record (log) is kept if taken		Essential	O	Certification is not given if record (log etc.) is not taken
	Security Patch Management	Patch update interval (time from vendor release to start of patch testing)		Essential	O	Certification is not given if management is not carried out
Network						
Lines	Recommended line	Type of line such as dedicated line (including VPN)and Internet Range of responsibility that ASP/SaaS should take for user connection line		Essential		
	Recommended band	Presence or absence of recommended band, level of recommended band if present		Essential		
	Recommended terminal	Type of devices such as PC and mobile phone, type of browsers to be used		Essential		
Security	Firewall	Presence or absence of firewall		Essential	O	Certification is not given if firewall is not present
	Network Intrusion Detection System	Presence or absence of detection mechanism of unauthorized server intrusion by illegal packet or non-privileged user		Essential		
	Network monitoring	Reporting time when a failure occurs in the network (dedicated line etc.) between enterprise and end user		Optional		
	Management of IDs and passwords	Presence or absence of standards of administration method of ID and password (although the content is not disclosed, submission of standards which describe administration method etc. is required as examination documents for certification		Essential	O	Certification is not given if standards are not present
	User authentication	Presence or absence of personal authentication (Web, serer) and user authentication by ID/password through authentication platform, method of authentication if present		Essential	O	Certification is not given if user authentication is not present
	Administrator authentication	Presence or absence of formal procedure to register/remove administrator privileges for server operator (although the content is not disclosed, submission of standards which describe procedures etc. is required as examination documents for certification)		Essential	O	Certification is not given if procedure is not present

	Defence against Spoofing	Presence or absence of measures taken for spoofing where a third party pretends to be a user company, method of authentication if present		Essential	O	Certification is not given if spoofing measure is missing
	Other security measures	Describe freely measures for information leak and data encryption.		Optional		
Housing (Location of servers)						
Building	Building for data centre or not	Whether or not the building is solely occupied by data centre		Essential		
	Location	Country name, regional block name (if Japan, e.g. Kanto, Tohoku)		Essential		
	Earthquake resistant structures	Earthquake resistance value Presence or absence of quake-absorbing structure or quake-damping structure		Essential		
Emergency electric power facilities	Uninterruptible power supply (UPS)	Presence or absence of Uninterruptible Power Supply (UPS), power supply duration if UPS is present		Essential		
	Power supply route	Whether or not 2 or more power supply routes via different substations are secured (except private power generator and UPS)		Essential		
	Emergency power supply	Presence or absence of emergency power supply (private power generation), continuous operating time value if emergency power supply is present		Essential		
Fire extinguishing systems	Fire extinguishing systems in the Server Room	Presence or absence of automated fire extinguishing system, whether or not it is gas-based fire extinguishing system if present		Essential		
	Fire sensor / alarm system	Presence or absence of fire detection system		Essential		
Protection against thunders	Protection against direct thunders	Presence or absence of measures for direct lightening stroke		Essential		
	Protection against induced lightning from thunders	Presence or absence of measures for induced lightening stroke, value of maximum endurable voltage if present		Essential		
Air conditioning facilities	Adequate air conditioning facilities	Description of air conditioning facilities (upward blowing air conditioning on the floor, individual air conditioning dedicated for computer)		Optional		
Security	Control of people's entry and leaving	Presence or absence of entry and leaving record, how long record is kept if present		Essential		
		Presence or absence or surveillance camera, operating hours and monitoring range of surveillance camera if present		Essential		
		Presence or absence of personal authentication system		Essential		

	Stock of recording media	Presence or absence of cabinet with key lock to keep medium such as paper, magnetic tape, and optical media Presence or absence of stock control procedure documents		Optional		
	Other security measures	Describe freely other notable security measures (breaking and entering prevention, monitoring for security etc.)		Optional		
Service support						
Service desk (Complaints desk)	Contact address	Contacts such as phone/Fax, Web, and email address		Essential	O	Certification is not given if point of contact is not present
	Business hours and dates	Business days and hours (open hours)		Essential		
		Maintenance time		Essential		
	Support	Availability rate of service support	○Service support availability rate =[actual work time of point of contact] / [service support open hours]	Optional		
		Abandon rate	○Abandon rate: rate at which operators did not answer incoming calls (operator busy)	Optional		
		Response time adherence rate	○ Response time adherence rate: ratio of calls answered by operators within a specified time against all calls	Optional		
		On-time completion rate	○On-time completion rate: ratio of calls completed within the time specified for each point of service or service type against all requested calls	Optional		
	Coverage / measures of support	Coverage of support Means of support (phone, Email etc.)		Essential		
Guarantee and continuity of the services	Structure to avoid service disruption	Structure to prevent service suspension (redundancy, load balancing etc.)		Essential		
	Liability and amount of the limit of the accident	Scope of liability of ASP/SaaS provider at accident occurrence and compensation coverage policy		Essential		
Notification and report of Services	Prior notice of temporary closures by such as maintenances	Time and method of prior notice to users (Describe time of prior notice using such units as 1 month prior, 3 months, 6 months, and 12 months)		Essential	O	Certification is not given if prior notice is not present

	Notification systems of accidents and disasters	Presence or absence of notification at failure occurrence		Essential	O	Certification is not given if notification at failure occurrence is not made
	Periodical reports	Presence or absence of regular reporting to users (monitoring results of application, server, platform, and other equipment, service availability ratio, SLA execution result etc.		Essential		