Information Disclosure Guidelines for Safety and Reliability of IaaS / PaaS

Condition 1: Objective of information disclosure

Information disclosure would be made in a unit of each IaaS/PaaS.

Condition 2: Definition of “IaaS/PaaS”

“IaaS/PaaS” is defined in this guideline as follows.

“IaaS (Infrastructure as a Service)” means services which offer hardware resources, such as servers, hard disks and storages, necessary for ASP, SaaS or PaaS. In a broader sense, it means services which include data centers. “PaaS (Platform as a Service)” means services which offer system resources, development and operation resources and network facilities in a narrower sense, while meaning services which include data centers and IaaS in a broader sense. IaaS and PaaS are collectively called hosting services.

Items for Information Disclosure		**Description**	**Essential / Optional**
Time of the Information Disclosure	Date of the Information Disclosure	Year, month, date of information disclosure (in Western calendar)	Essential
Place of business enterprise / Business			
Business enterprise Overview	Name of business enterprise	Formal name of business enterprise (trade name)	Essential
	Website of business enterprise	URL of homepage of business enterprise	Optional
	Established Year / Years in Business	Established year of business enterprise (in Western calendar)	Essential
		Years in the business	
	Office (enterprise place)	Address, postal code of head office of business enterprise	Essential
		Number of offices (domestic, overseas)	
Business overview	Principal business overview	Overview of principal business of business enterprise	Essential
Human resources			
Management	Representatives	Name of representative	Essential
		Background of representative (age, academic, career, certificate etc.)	Optional
	Executive	Number of executive	Optional
Employees	Number of employees	Number of regular employees (single basis)	Optional
Financial Conditions			
Financial Data	Sales	Sales of the entire business enterprise (Consolidated base) (unit: Yen)	Essential
	Ordinary profit	Ordinary profit of the entire business enterprise (Consolidted base) (unit: Yen)	Optional
	Capital	Capital of the entire business enterprise (Consolidated base) (unit: Yen)	Essential

	Equity ratio	Ratio of equity capital of the entire business enterprise (Consolidated base) (unit: %)	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; (1) accounting audit by accounting auditor, (2) audit by accounting adviser, (3) financial data based on checklist according to small and mid-sized enterprise accounting, or (4) none of the above	Optional
	Mandatory publication of financial statements	Whether or not financial statements 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	Main dealing financial institution	Name of main dealing financial institution	Optional
	Name of industry and/or non-governmental organizations which enterprise belongs	Names of industry organizations, economic organizations and others which enterprise belongs	Optional
Compliance			
Organization-system	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 documents such as basic policies, organizational rules, manuals etc. on the information security, names of documents if present	Essential
		Whether or not the above documents are approved by managements	
	Policies on the complaint procedure relating to IaaS / PaaS	Presence or absence of documents such as basic policies, organizational rules, manuals etc. on the complaint procedure relating to IaaS /PaaS service, names of documents if present	Essential
		Whether or not the above documents are approved by managements	
	Policies on the Business Continuity	Presence or absence of documents such as basic policies, plans, manuals etc. on business continuity, names of documents if present	Essential
		Whether or not the above documents are approved by managements	
	Policies on the Risk Management	Presence or absence of documents such as basic policies, plans, manuals etc. on risk management, names of documents if present	Essential
		Whether or not the above documents are approved by managements	
Basic features of services			
Service overview	Name of services	Name of IaaS/PaaS service that disclosed information	Essential
	Start date of services	Year, month, date of service launch of IaaS/PaaS service that disclosed information (If major renewal has occurred between service launch and application, sate year, month, date of the renewal)	Essential
	Basic types of services	Select appropriate type from the following; system platform service, development/runtime platform service, application platform service, hardware platform service, or network platform service	Essential
	Limitation on service customization	Range of application customization (It not defined or to be discussed separately, describe so)	Essential

	Types of lines and bandwidths	Type of line such as dedicated line (including VPN)and Internet Type of band provided, description of band guaranty if present	Optional
Structure of services (System PaaS)	Provided OS	Presence or absence of provision of virtualized OS Describe OS that serves as single OS (Windows, Unix, Linux, etc.)	Essential
	Server maintenance	Description of services such as server OS initialization, patch update for OS, etc.	Essential
	ASP / SaaS Support services	Description of services such as search, authentication, clearing/billing, security, location data, timestamp, media, language conversion, etc.	Essential
	Network provision for the connections by administrators	Description of access methods such as remote desktop, SSH, etc.	Essential
	Backup and restore services	Description of backup service, restore service at system failure, etc.	Essential
	Other services	Description of administrative application service, clearing service, representative service, consulting service etc.	Essential
Structure of Services (Development and execution PaaS)	Support services for software development	Provision of Java, Servlet, Perl, PHP, Ruby, C/C++ and other open source development environments etc.	Essential
Structure of Services (Application PaaS)	Services for domain name management	Description of services for IP address management, domain acquisition/management, DNS server management, etc.	Essential
	Mail Services	Description of services for Web mail, mailing list, etc.	Essential
	Web Services	Description of services for Web server, FTP server, Web account, access control, access log analysis, access log acquisition, blog, BBS etc.	Essential
	Others	Description of services for API, DB server, etc.	Essential
Structure of Services (Hardware PaaS)	Server services	Description of services for shared server, dedicated server, etc.	Essential
	Storage services	Description of storage hosting service	Essential
	Rental equipment services	Presence or absence of trouble-shooting service, regular operation service, operation/maintenance support service for rental equipments, description of services if present	Essential
	Services for integrated resource	Description of services offered by integrating virtual resources (virtual machine, server, storage, network etc.)	Essential
Structure of Services (Network PaaS)	Load balancer services	Description of load balancer service	Essential
	Network device services	Description of services to provide network equipment such as router, switch, etc.	Essential
Quality of Service	Service availability	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	Essential
	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 of technical measure (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 (JIS Q 27001 etc.), ITSMS (JIS Q 20000-1 etc.), presence or absence of audit report created upon ASCR18 (SAS70 in US). Provide 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	Presence or absence of vulnerability assessment Readiness of assessment criteria and procedure to take countermeasure, outline of state of countermeasure taken	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	Essential
	History of award or commendation	History of awards received relevant to IaaS/PaaS service	Optional
	Service level agreement (SLA)	Whether or not SLA relevant to this certification items is attached to contract	Essential
Change / termination of services	Prior notice of the change or termination of services	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
	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
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 * Details such as price chart for each service can be attached as appendix	Essential
	Method of payment	Methods of payment such as credit card payment, electronic money payment, etc.	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
Amount of services used	Number of users	Number or user licenses for IaaS/PaaS service that disclosed information (identify if this is the number of concurrent users or actual users)	Optional
	Number of agencies	Number of agency of IaaS/PaaS service that disclosed information	Optional

Data Management	Location of the data	Location of saved customer data (place where data exists) when IaaS/PaaS service is provided (describe country name)	Essential
	Data center used	Number of data centers used when IaaS/PaaS service is provided	Essential
System Operation (Operation of PaaS, Security)			
Operation of PaaS	Live-or-death monitoring	Presence or absence of live-or-death monitoring, monitoring target if live-or-death monitoring is carried out (platform, storage etc.), and monitoring interval, monitoring time, notification time of each live-or-death monitoring target	Essential
	Fault monitoring	Presence or absence of fault monitoring	Essential
	Time Synchronization	Method of time synchronization of system	Essential
Security (Platform, Storage)	Anti-virus measures	Presence or absence of antivirus measure, if present, update interval of pattern file (time from vendor release)	Essential
	Administrator authentication	Presence or absence of formal procedure to register/remove administrator privileges (although the content is not disclosed, submission of standards which describe procedures etc. is required as examination documents for certification)	Essential
	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
	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
	Security Patch Management	Presence or absence of standard that defines how to acquire security patch information, assessment method, decision criteria, update procedure, update interval at normal time, emergency response, etc.	Essential
Security (Network)	Firewall	Presence or absence of firewall	Essential
	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 contract user	Optional
	Virus check	Presence or absence of measures to email, download file, and access to files on servers, update interval of pattern file (time from vendor release) if measure is present	Essential
	User authentication	Presence or absence of personal authentication (Web, server) and user authentication by ID/password through authentication platform, method of authentication if present	Essential
	Record (Log)	Network usage, whether or not record of exception handling and security event (log etc.) is taken, how long record (log) is kept if taken	Essential
	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
	Other security measures	Describe freely measures for information leak and data encryption.	Optional
Housing (Location of servers)			
Building	Name of data center	Formal identification name or abbreviated name of the data center indicated in the above item No, 75 <*> * the term abbreviated name here means “A, B, C...” or “1, 2, 3,,,” etc.	Essential
	Beginning year of the Data center	Year from which data center began its business	Essential
	Building for data centre or not	Select whichever is closer between building dedicated to data center and office building	Essential

	Location	Country name, regional block name (if Japan, e.g. Kanto, Tohoku)	Essential
		Describe notable geographical advantages if any (e.g. altitude, ground condition etc.)	Optional
	Earthquake resistant structures	Earthquake resistance value (seismic intensity)	Essential
		Building structure relevant to earthquake measures (quake-absorbing structure, quake-damping structure etc.)	
Electric power facilities	Uninterruptible power supply (UPS)	Presence or absence of measures to establish uninterruptible power supply (UPS installation etc.), minimum power supply duration if present, and relevance with start-up time of emergency power supply	Essential
	Power supply route	Whether or not 2 or more power supply routes via different substations are secured (except UPS and emergency power supply)	Essential
	Emergency power supply	Presence or absence of emergency power supply (private power generation), continuous operating time without refuelling if present, and description of emergency power supply operation measure (method of continuous fuel supply etc.)	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 (whether it is halon gas type or new gas type) if present	Essential
	Fire sensor / alarm system	Presence or absence of fire detection system and smoke 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 (optional)	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, water-cooling/air-cooling, other devices etc.)	Essential
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 of surveillance camera, operating hours and monitoring range of surveillance camera, how long videos are kept, and availability of alternation prevention feature if present	
		Presence or absence of personal authentication system	
	Stock of recording media	Presence or absence of cabinet with key lock or stock room to keep medium such as magnetic tape, optical media, etc.	Optional
		Presence or absence of stock control procedure document	
	Other security measures	Other notable security measures	Optional
Service support			
Service desk (Complaints desk)	Business hours and dates	Business days and hours (open hours)	Essential
		Availability of outside hours response	
	Coverage / measures of support	Support coverage	Essential
		Contact method (phone/Fax, E-mail etc.)	
Guarantee and continuity of the services	Liability and amount of the limit of the accident	Presence or absence of document stating liability of data center provider at accident occurrence and compensation coverage policy, name of document if present	Essential

Notification and report of Services	Prior notice of temporary closures by such as maintenances	Time 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
		Methods of prior notice to users	
		Presence or absence of emergency maintenance with shorter notification period than described above	
	Notification systems of accidents and disasters	Presence or absence of notification at failure occurrence	Essential
	Periodical reports	Presence or absence of regular reporting to users	Essential