Terms & Conditions of Use of EP-BB (between the Service Provider and User)

1. Definitions

1.1 "Electronic Partnership", "EP" or "EP-BB" refers to the system to collect relevant information from the Device (as hereinafter defined) located in premise of the customer (hereinafter referred to as "User") and to provide various services through electronic communications ("Services").

1.2 "EP Center" refers to the servers operated by FUJIFILM Business Innovation Corp. ("FB") for collecting relevant information from the Device.

1.3 "Device" refers to the multi-function devices or printers that are designated for EP by User, in accordance with the service application form prescribed by the Service Provider (hereinafter referred to as "Service Application Form").

2 EP Communication Equipment Built-in Device (EP-BB):

User acknowledges that EP-BB communication equipment which is built in the Devices, connect to the network environment (LAN) of User and send information to EP Center via Internet.

3. Agreed terms of Use:

3.1 User agrees the Service Provider, its outsourced service providers and FB may use the User's information in EPBB Service Application Form for the following purposes:

(a) To provide various Services to User via EP;

(b) To communicate with User regarding the provision of various Services via EP if necessary;

(c) To send EP relevant materials to User upon request;

(d) To provide Device information to User;

(e) To promote marketing activities to User, including surveys for improving the quality of products or services provided to User by the Service Provider.

3.2 Details are as follows:

Purposes of use	Information collected
・ Automatic remote reading of Device meter count ・ Expense charge according to the read meter count ・ Remote maintenance of Device ・ Delivery of Device supplies ・ Quality improvement of Device ・ Various proposals from the Service Provider to User	・ Device identifier (model name, serial number, etc.) ・ Various meter count values of Device ・ Supply information of Device supplies ・ Device information for automatic monitoring and diagnosis of troubles encountered by Device

3.3 The Service Provider shall not use nor disclose the information collected for other purposes, except for those which are expressly permitted by User. To the extent that FB processes personal information on behalf of a Data Controller falling under the jurisdiction of the EU GDPR (General Data Protection Regulation 2016/679, FB undertakes to process the data in accordance with the provisions set out in the attached Exhibit 2 (EU Data Processing Agreement).

3.4 User acknowledges that the Service Provider may fail to obtain information via EP in following situations:

(a) The electrical power to the Device is switched off, or communication with EP Center has failed due to any reasons.

(b) Network communication is blocked due to any reasons.

(c) EP management system is suspended for maintenance or other operations.

(d) Any other technical faults.

3.5 User agrees to appoint such individual stated as "Contact Person" in Service Application Form as its authorized person, for all matters related to the EP. If there are any changes to the "Contact Person" details, the User shall notify the Service Provider in writing within 10 working days prior to such changes, failing which the User shall be liable for all losses or damages arising directly or indirectly from such failure to notify.

3.6 The Service Provider and FB do not warrant that the operation of Services shall be uninterrupted or error free, or that all defects can be corrected.

To the extent permitted by law, neither party shall be liable to the other party for any damages arising out of or relating to EP or the Services (including without limitation to loss of revenue, loss of profits, loss of computer, server or any equipment or software, usage time, and damage or loss of use of data), even if the party has been advised of the possibility of such damages, and irrespective of whether such damages result from a claim arising under tort or contract law

4. User shall maintain EP connection environment as follows.

(a) It is the User's responsibility to maintain the required connection environment for the communication between the Device and EP Center

(b) Any expenses incurred in relation to power supply, circuit works regarding EP connection environment maintenance and any other expenses shall be borne by User.

(c) In the event that User wishes to change the setting of Device

which has been installed with EP communication device, User shall give prior notification to the Service Provider.

5. User acknowledges that the security features of EP-BB are as follows.

5.1 The communications of EP-BB via Internet are protected by digital certificates for rigid client authentication.

5.2 The communications between EP-BB and EP Center are encrypted with SSL to prevent data wiretap or manipulation. EP Center will send a certificate to EP-BB to prevent illegal access.

5.3 For EP-BB, any access of Device from the EP management system site is prohibited. EP relevant system setting information can only be changed by polling, when there is a notification by the Device.

6. Variation

The Service Provider shall have the sole discretion to amend the terms and conditions of use at any time, without notifying the User. If, in a reasonable opinion of the Service Provider, such terms and conditions may cause a material impact on User, the Service Provider may notify the User of such amendment beforehand.

7. Charges

The Service Provider reserves the right to charge the User for the provision of any Services rendered via EP with one (1) month's prior notice.

8. Termination

Either the Service Provider or User may cease using EP after giving the other party 4 week's prior written notice.

9. Disclaimer of Warranty

User acknowledges that EP is provided "as is". The Service Provider and FB disclaims any representation warranties, including but not limited to the merchantability, fitness for a particular purpose or non-infringement of third party's intellectual property rights.

Notwithstanding any of the foregoing, if the User finds any failure of meter counting for auto-billing via EP with reasonable evidence, User may request the Service Provider to correct such meter count.

10. Limitation Liability

Neither party shall be liable for any direct or indirect, incidental, special punitive or consequences damages, or any loss of data or use.

11. Governing Law

The terms and conditions are governed by the laws of the country where the Service Provider is based.

12. Jurisdiction

Any and all disputes, controversies and differences arising between the parties out of or in relation to this terms and conditions shall be subject to the exclusive jurisdiction of the court where the Service Provider is based.

Exhibits

1. Terms & Conditions of Use for Firmware Update Service
2. Data Processing Agreement

Exhibit 1 to the Terms & Conditions of Use of EP-BB (between the Service Provider and User)

Terms & Conditions of Use for Firmware Update Service

1 Firmware Update Service ("Service") is a service that updates device's firmware to the latest version via Internet. Service is provided to customers ("User") by the following method: direct operation of the Device by User, or remote or direct operation of the Device by Service Provider or FUJIFILM Business Innovation Corp. ("FB").

2 “Device” refers to the multifunction devices or printers that are located in premise of the User, which is specified in the application form prescribed by Service Provider (hereinafter referred to as “Application Form”)

3 If you do not need Service, please contact your Service Provider.

4 User acknowledges and accepts the following precautions / restrictions for the use of Service.

(1) The data size of the firmware downloaded per Device by Services is as shown in Appendix. Depending on User's network environment, it may interfere with other communication. Therefore, sufficient communication bandwidth must be secured.

(2) Service may not support Device with the prescribed configurations or located in prescribed restricted areas.

(3) An estimate of the time required for updating the firmware is shown in Appendix.
Do not turn off Device until the update is completed.

(4) When Service is executed, Device sends the update request and firmware version information, but it does not send any personal information, nor the copy/print/fax/scan information stored on Device’s hard disk.

(5) While Service is running, all functions, including sending and receiving faxes from Device, will be stopped. Please note and acknowledge that User do not turn off the power or unplug the power outlet to avoid Device failing to boot.

(6) If any of the following problems occur, please contact Service Provider.

① Depending on Device firmware status, Service may not be available, or Service may fail to update firmware. In this case, a warning sign will be displayed on device control panel.

② On rare occasions, error message will be displayed on device control due to the failure of the firmware update.

(7) Service may not be provided due to periodic maintenance of FB server.

5. The Terms and Conditions of Use may be changed at any time without any prior notice to User if deemed necessary by Service Provider. After the change, the revised Terms and Conditions of Use will apply.

※

※

※

※

※

※

※ ※ Firmware and its data size may be changed to improve the quality of Device.

Date of revision: April 1, 2022

Appendix to the Terms & Conditions of Use for Firmware Update Service

(The data size of the firmware downloaded per Device)

The data size of the firmware downloaded per Device can be up to approximately 550MB.
Approximately 4 to 15 minutes are required between the start of firmware download and completion of firmware update. (Download Internet speed 1.5MB/s)

※ The above time is a reference value.
The download time is affected by the network environment.

※ The above data size of the firmware downloaded per Device is for the model that supports the Service as of February 8, 2022.

※ Firmware and its data size may be changed to improve the quality of Device.

Exhibit 2 to the Terms & Conditions of Use of EP-BB (between the Service Provider and User)

Data Processing Agreement pursuant to Article 28 GDPR (EU)

Section I

Clause 1 - Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to III are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 - Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 - Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

Section II - OBLIGATIONS OF THE PARTIES

Clause 6 - Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 - Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least four weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 - Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 - Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under [Articles 33 and 34 of Regulation (EU) 2016/679.

Section III - FINAL PROVISIONS

Clause 10 - Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I - List of parties

Controller(s)

The “User” as defined in the Preamble to the Terms & Conditions of Use of EP-BB

Processor(s)

FB, Service Provider and its outsourced service providers as defined in the Preamble to the Terms & Conditions of Use of EP-BB

ANNEX II - Description of the processing

1.	Categories of data subjects whose personal data is processed	Controllers clients' data, internal Controller data relating to employees and other third parties.
2.	Categories of personal data processed	Personal identifiers including name and address, and other personal data.
3.	Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures	none
4.	Nature of the processing	Accessing equipment where personal data may be stored when performing support and maintenance services for the Customer.
5.	Purpose(s) for which the personal data is processed on behalf of the controller	Delivery of equipment, installation, acceptance, support, maintenance and repair.
6.	Duration of the processing	For the duration of the provision of the Services.
7.	For processing by (sub-) processors, also specify subject matter, nature and duration of the processing	Support, maintenance and repair.

ANNEX III - Technical and organisational measures

FB shall at least implement the technical and organisational measures specified in this Annex to ensure the security of the personal data.

1. Scope

1.1. This Annex sets out FB's key responsibilities concerning the security requirements for the IT environments, facilities and personnel used to create, develop, and manage the services provided.

1.2. This Annex and the requirements set forth herein are in addition to, and not in lieu of, other requirements incorporated into the Principal Agreement. The requirements of this Annex apply to FB as well as its subcontractors, and FB shall be fully liable for the performance of its subcontractors.

2. General security requirements

2.1. FB will provide Services which are designed, delivered, and at all times support compliance with industry standards and best practices, such as ISO 27001 for Information Security.

2.2. FB will independently and proactively follow industry developments and endeavour to incorporate the newest approved best practices into its day to day operations.

3. Security management

3.1. Security responsibilities within the organization is assigned by senior management to nominated individuals. The responsibilities include overall security, risk management, privacy, and controls for handling Personal Data. FB have a documented process for reviewing the implementation of security within its organization.

3.3. By obtaining and complying with ISO 27001, FB establish and maintain a security architecture which provides a framework for the standard security controls throughout FB organization.

3.4. FB have comprehensive, documented information security policy and related guidelines. The information security policy is approved by senior management.

3.5. FB adopt and document security measures for information systems and the creation, use, modification, and deletion of data in the "Information security regulation". Also we have "Global Classified Information Management Regulations" which prescribes information classification scheme..

3.6. FB implement and regularly update a security risk management system, which incorporates emerging threats, possible business impacts, and probabilities of occurrence. FB will modify security related processes, procedures, and guidelines accordingly. Security is monitored by the Security Operation Center, and if a threat occurs, it is handled by a cross-organizational cyber security incident response organization (CERT).

3.7. FB will maintain system documentation in adequate level until the end of the Service lifecycle. Upon expiry or termination of the Agreement, FB will, unless otherwise agreed in the Agreement securely delete the data upon Company's instruction. Upon Company's request, FB will confirm secure deletion of all data in writing signed by a duly authorized representative within thirty days from the receipt of such request.

4. Audit rights

4.1. FB will detail in Service Platform Security Whitepaper, how Company related data is protected to ensure that Company's data security, privacy and other compliance requirements are met.

4.2. On a regular basis FB will carry out external audits on ISMS on the FB's compliance with this Annex. Visibility of the assessment results will be provided to Company, including at the minimum the scope of the assessment, security findings and their mitigation status. FB will immediately report any critical vulnerabilities or findings to Company.

4.3. Company (or an independent Third Party appointed by Company) may conduct an audit of FB according to an audit plan upon five (5) calendar days' prior written notice. Company may also request to audit FB's subcontractors respectively. Additionally, Company or its designated security auditing partners may perform ad hoc testing and application security reviews of any service that is about to be deployed or that is currently operated by FB. Company strives to inform FB five (5) calendar days in advance of such testing and reviews.

4.4. Company is responsible for the costs of the reviews and tests referred to in section 4.3. However, should the testing or review reveal any violation or breach of this Annex by FB, FB shall compensate Company for the reasonable costs arising from the audit and remedy the breach.

4.5. If the audits, reviews or assessments reveal any violation or breach of this Annex by FB, FB will without delay remedy the breach without any cost to Company.

4.6. When Company requests all policies, guidelines, plans, systems, schema, and methodologies set forth in this Annex, FB will report on the status of incidents that affect Company. FB will provide various documents related to system specifications and service operation specifications.

4.7. FB will provide Company visibility on where Company related data is processed, stored, transmitted, and where it may be accessed from. FB will inform Company in writing in advance should FB intend to transfer Company related data to another location and obtain Company's prior written consent for such transfer.

5. Incident handling & response

5.1. FB will have adequate and documented issue/incident response procedures and nominated persons to timely react and prevent any further damage caused by security, privacy or any other compliance issues, vulnerabilities, or incidents.

5.2. FB will inform Company without delay in case of any Company related security incident.

5.3. FB will at all times maintain the capability to prevent, monitor, detect, investigate and respond to security and privacy incidents.

5.4. FB have proper forensic procedures in place to ensure chain of custody, which is required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident.

5.5. FB will maintain capability to detect potentially suspicious network behaviours and/or file integrity anomalies and capability to support forensic investigative capabilities in the event of a security breach.

6. Business continuity

6.1. FB have a service continuity plan and an initial guide in the event of a disaster. FB will demonstrate the functioning of such plans by conducting regular tests and exercises. At Company's request, FB will provide reports on the tests and exercises it has undertaken to verify its ability to recover from a realized risk event.

6.2. FB will also facilitate the recovery of information assets through a combination of preventive and recovery controls. Said controls shall be in accordance with applicable statutory, regulatory, and legal requirements and consistent with industry standards and best practices. The availability requirements are 1) Recovery Time Objective: Within 2 hours and 2) Recovery Point Objective: 1 day before the failure

6.3. FB will enforce a documented backup policy that ensures the capability to fulfil agreed Service Levels and continuity requirements during emergency situations. The backups will be stored in secure storage. Actual restoration of the backups will be tested regularly to ensure their usability.

6.4. FB will store backups of Company related data based on the criticality of the data. FB will store daily database backup for last 7 days, and daily storage backup for last 1 day.

7. Personnel security and awareness

7.1. FB ensure that its employees and subcontractors are bound by statutory or contractual confidentiality obligations prior to accessing Company related data. Employees have a written oath when they join the company. The contractors are supplemented by contracts.

7.2. FB will maintain an appropriate entry and exit procedure for personnel changes that includes disabling user access rights upon termination of employment with FB or termination of assignment for Company.

7.3. FB conduct security and privacy awareness training for at least annually for all existing employees and new hires performing Services for Company. Due emphasis shall be given to client confidentiality, understanding the agreed confidentiality obligations and specifically the sensitivity of personal data. Advanced security training will be given to key roles (e.g. administrators or employees with full access to Company related data) working with sensitive information and assets (e.g. Company data, financial data or employee data).

7.5. FB undertakes to use only properly screened employees and/or subcontractors to fulfil its obligations towards Company. Depending on the nature of the services provided by FB, Company reserves the right to request proof of proper screening of the relevant employees of FB or an ISO-27001 certification of FB.

8. Physical security

These physical security requirements apply only to data centres, assuming that Company related data is fully encrypted in the premises where it is processed and it is not extracted (e.g. laptops fully encrypted, data never printed). Refer to the information published by Amazon Web Services for physical security of data canter. https://aws.amazon.com/jp/compliance/data-center/controls/

9. IT security

9.1. FB will implement information security measures to protect Company related data against unauthorized or accidental access, use, disclosure, deletion, loss, alteration or amendment. Company related data will only be stored and processed in an environment where security and privacy controls have been implemented.

9.2. FB will logically isolate all Company related data from its own and all of its other customers' data so that Company related data is processed, transmitted, accessed and stored by a minimum number of authorized persons who only have access to such data that they need to perform their work related duties (role-based access control). This concerns also backups and logs.

9.3. Identity and Access Management for development and administrative purposes must fulfil at least the following requirements:

(a) FB will have policies for approving, creating, and terminating user access rights

(b) FB shall have policies and/or guidelines for strength and rotation of access credentials, e.g.

(1) Implementing an automatic and forced password resetting process

(2) Prohibiting and preventing the use of default or weak passwords

(3) Securely handling and delivering credentials (such as user name and password)

(c) Every user must be individually identifiable. Common/shared user accounts are prohibited and the use of them shall be prevented

(d) Any credentials must have the minimum permissions required for their intended use

(e) As part of software development two-factor authentication shall be implemented based on threat analysis. In case of administrative remote access to environment with Company related data two-factor authentication is always required

9.4. FB will ensure that there is a sufficient audit trail of the use of access privileges (changes, who, what, when) in place for Company related data. Logs regarding user access and all activity that creates, changes or deletes Company related data will be collected and stored for 12 months, if required by statutory, regulatory, or legal obligations. Access to log data shall be restricted to prevent compromise and misuse of log data. Company shall have right to know who has access to its data. FB will support Company in case of security investigations or requests from authorities by providing visibility to relevant logs.

9.5. FB will protect at FB's own premises and/or systems, all Company data by appropriate controls including, but not limited to network segmentation using host based firewall or network based firewall, firewall log monitoring, network intrusion detection or prevention systems (IDS/IPS), web application firewalls, log management, correlation capability, malware prevention for servers and end-user computing devices, application and infrastructure vulnerability scanning. FB will maintain documented processes to ensure that all network devices are protected from unauthorized access and that all updates are conducted based on an agreed maintenance plan.

9.6. FB will deploy any host systems using a standardized secured configuration (hardened, i.e. provide only necessary ports, protocols, and services to meet the functionality requirements). Sufficient vulnerability and patch management processes will be maintained and followed in order to implement security patches and fixes in a timely fashion according to industry best practices and the level of criticality.

9.7. Sharing of Company related data will only be undertaken through secure data sharing portals or tools. The use of insecure file transfer protocols is strictly forbidden.

9.8. FB will maintain TLS certificates needed to provide the Services, and monitor the expiry of all TLS certificates, and manage their timely replacement.

9.9. FB will encrypt all information and/or data by using current industry-standard strong encryption, key management and related standards, when processing, transmitting and/or storing personal data, consumer data, Company confidential or secret information in public cloud environments, including consumer cloud storage services and transmission of data over the public Internet.

9.11. FB will establish policies and procedures and implement mechanisms for effective key management to support encryption of data in storage. Key management and key usage shall be separated duties.

9.12. FB have remote access and remote work policies, practices, guidelines, and restrictions in place.

9.14. All laptop hard disks and other client devices (like USB-memory sticks, netbooks, smartphones, tablet computers, portable media players, etc.) and other removable/back up media containing Company related data will use full data encryption.

9.15. FB will securely and permanently destroy/wipe Company related data in a Company-approved manner from all media and/or devices when it is no longer required for the Services. Any old or broken media containing Company related data will be effectively and permanently wiped without possibility to retrieve any data or destroyed prior to being decommissioned or reused. FB will ensure that necessary backup arrangements are taken into account prior disposal.

9.16. Workstations and other end-user devices that are used to access Company related data will be installed from standardized installation images or by using standardized installation or configuration procedures. Devices will be configured to be resistant to attacks in accordance with industry standards and best practices and the means of connecting to networks, IT services or other end-user devices will be designed to be secure, and protected against unauthorized disclosure or alteration of business information. All software used in workstations will be regularly patched and personal firewalls shall be in use.

9.17. All and any device used or added to the end user environment (e.g. Bring your own device - BYOD) will be approved, protected by appropriate security controls and supported by standard operating procedures or instructions for acceptable use.

9.18. Automated, up-to-date and functional malicious code protection (such as an antivirus and anti-spyware/malware) will be installed in all systems used to deliver end-to-end service for Company.

9.19. Operational systems and software will be subject to strict change management control. Change management procedures (including changes to security features) will be agreed in the Security Governance.

9.20. FB will not process production data in non-production environments, unless relevant security and privacy controls as set forth in this Annex have been implemented to the non-production environment.

9.21. The use of administrative tools capable of potentially overriding system, object, network, virtual machine and application controls will be restricted.

9.22. FB will use a registered own mail domain account for email communication with Company and will not use generic free mail accounts.

10. Security and privacy by design

Security requirement confirmation rules for software quality inspection or change management within the infrastructure are defined and implemented accordingly.

10.1. IT system development activities will be conducted in accordance with a documented system development methodology, which includes the requirement for information security measures at each stage of the system development lifecycle.

10.2. FB will design and implement all its products and Services delivered to Company properly taking into account relevant privacy and security related requirements (e.g. privacy and security by design). This means in practice that for any new or changed functionality FB will conduct:

(a) architectural/design threat analysis and for identified risks define which controls are to be implemented and which risks will be treated in some other jointly agreed way

(b) security and privacy assessment (e.g. internal/external audits or testing) for features that have been flagged as a risky area in threat analysis, or are a part of a security or privacy control

(c) Architectural/design threat analysis should be based on data flow diagrams and cover at the minimum but not limited to:

(1) Identity and access management

(2) Impacted user experience/business logic flows

(3) Impacted personal data flows

(4) Software dependencies (e.g. third party components, libraries)

(5) Deployment architecture

(6) Software development pipeline

(7) Auditability (e.g. logging)

(8) Service/Product lifecycle until retirement

10.3. Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g. OWASP Top 10 for Web Applications and OWASP ASVS for testing coverage) and adhere to applicable legal, statutory, or regulatory compliance obligations.

10.4. On Company's request FB shall provide visibility of the identified risks, threats and assessment results.

10.5. FB shall include security controls such as:

(a) secure coding standards/guidelines

(b) change controlled configuration

(c) third party components vetting and vulnerability management

(d) security tests that establishes that each of the security requirements has been met

(e) apply, test, and validate the appropriate patches and updates and/or workarounds

(f) ensure that all security issues shall be evaluated and fixed based on risk analysis.