

Form No	F010-BYOD-UT01	Reference	ISO/IEC 27001:2013
Document ID	ISMS/8.1/F010	Reference Section	8.1.2

## **BYOD UNDERTAKING**

As and where necessary, company will allow mobile devices like mobile phones, tablets or personal laptops to be connected to company's network and computer systems, for conducting day to day work, software development and testing etc. However the access will be secured and regulated to ensure confidentiality and integrity of company data and information stored on individual's device.

This document extends to all employees, associates, consultants of the Bankai Group of Companies and is deemed to be incorporated in the service conditions of all employees requiring BYOD access.

***This undertaking document describes general guidelines for this section, which may be updated & changed as per Company's requirement. The last update version of Policy, Process or Undertakings, will automatically apply to previously accepted documents.***

### **1.1 General guidelines**

The general guidelines pertaining to this section are as below

- All mobile phones whether provided by company or owned by individual will be authorized to connect to company network and computer system, based on approvals from HOD.
- HODs shall approve access to mobile devices connections basis the legible reasons like day to day work, software development and testing etc.
- Employee who are granted to being own laptops, tablets under BYOD policy need to adhere to all policies related to company's ICT infrastructure.
- For BYOD devices, company may ask employee to provide access of device to ICT for installing various application for productivity, security, antivirus, data loss prevention, monitoring etc.
- For BYOD devices, company will maintain Administrative access to Laptops, Tablets, Desktops etc. for day to day management, administrative control, policy enforcement etc. , till the time BYOD device is approved for use in Company's network / IT infrastructure.
- Company may implement tools like Mobile Device & BYOD Management (MDM etc) to improve security and management of it's ICT infrastructure and environment.
- Company reserves rights to monitor activities performed through mobile or BYOD devices and take notice of any unwanted, suspicious and harmful activities. Company may take administrative or legal action in case of any such observations.
- ICT will remove all Administrative access, License Software, Productivity tools, IT Management tools, etc. provided by company under BYOD access , due to change of status of device from BYOD to personal use or at the time of exit of employee.

### **1.2 Employee responsibilities**

Each employee who has been granted mobile device or BYOD connection to company network & computer systems;

Form No	F010-BYOD-UT01	Reference	ISO/IEC 27001:2013
Document ID	ISMS/8.1/F010	Reference Section	8.1.2

- Must ensure that they are using access for day to day work and business only.
- Must adhere to all policies and guidelines contained in this or any other policy document, released by company.
- Shall provide access to their device for installing mandatory and recommended applications like Antivirus, Security, DLP & monitoring shall be installed on BYOD devices.
- Any licensed application software will be installed on BYOD devices based on HOD's approval only.
- Employee shall provide access to such devices in use for data integrity and security checks.
- Employee shall be responsible for upgrades, accessories, repairs etc. required for BYOD device operations.
- Employee shall inform ICT and respective HOD if BYOD device is being converted to non-BYOD devices and being taken back for personal use.
- Employee shall handover all company data, information, access to remove company provided applications and software, data wiping etc. at the time of converting BYOD device to non-BYOD or disengagement with company.

### 1.3 Loss or Damage of BYOD Asset

- Employee is primarily responsible for upkeep, maintenance, loss or damage of BYOD asset permitted for official use. However following guidelines will be referred on time to time basis
- Company is not responsible for upkeep, maintenance, loss or damage of BYOD assets permitted to employee for official use.
- Company is not responsible for any loss or damage, which happens due to negligence of employee.
- Company is not responsible any direct /indirect circumstances which caused damage to BYOD device at office premise. Example rain, electrical problem, fire etc.
- Loss or damage of BYOD asset due to negligence of company staff, other than BYOD owner will be subject to joint review of events by HOD, HRD & other company officials and reserve right to make the final decision on full replacement / partial replacement etc. of assets to the employee

#### By signing below, I agree to the following terms:

I have received and read a copy of the "Information Security Policy" and "BYOD Undertaking" and understand the same;

I understand and agree that any computers, software, and storage media provided to me by the company contains proprietary and confidential information about Bankaigroup and its customers or its vendors, and that this is and remains the property of the company at all times;

I agree, that I will share all necessary information required by ICT or other departments for processing, record keeping, references etc. of BYOD devices

BYOD UDERTAKING - May 2019

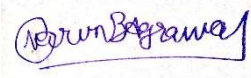



Form No	F010-BYOD-UT01	Reference	ISO/IEC 27001:2013
Document ID	ISMS/8.1/F010	Reference Section	8.1.2



I agree that I shall not copy, duplicate, otherwise disclose, or allow anyone else to copy or duplicate any of company's information or software;

I agree that, if I leave Bankaigroup for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, computer equipment, test devices or other equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.

Employee Signature		HOD Signature	
Employee Name	Varun Agrawal	HOD Name	Mark
Designation	Jr Developer	Designation	CGO
Date	26/04/2024	Date	30/04/2024
Department	Liferay PEG	Department	Corporate

**For ICT Use Only:**

ICT Engineer Signature		Device Activation Date	26/04/2024
ICT Engineer Name	Ravi Limbachiya	Admin Access Creation	YES
Date	27-04-2024	Record Update	

**List of Licensed Software Installed on BYOD Device:**

Device Inspection	Details	Name of License Software Installed by ICT
Make	Dell	Antivirus
Model	Latitude 5480	
Serial No/Service TAG	JBYP9H2	
Date of Purchase		
Warranty Status as on Date	Warranty Expired in 2020	
Accessories (adapter, mouse etc.)	<b>Charger S/N</b> : CN-06TM1C-LOC00-237-6A96-A12 <b>Mouse</b> : Dell (Wired Mouse) <b>S/N</b> : CN-OTW32R-LO300-80-066Q	<b>HostName</b> : Varun_Agrawal
Any Damages Observed	No	