OFFICE CIRCULAR NO. 26-002

Series of 2026

Guidelines on the Implementation of the Four-Day Onsite Work, Work-From-Home Friday Arrangement and Energy Conservation Measures Pursuant to Office of the President Memorandum Circular No. 114, s. 2026

SECTION I. RATIONALE

Pursuant to the directive of the President of the Republic of the Philippines implementing a Four-Day Workweek (4DWW) as part of a government-wide austerity and energy conservation measure, and in accordance with the authority granted under applicable civil service laws, rules, and regulations, this Office Circular is issued to prescribe the revised and updated guidelines for the proper and orderly implementation of the Four-Day Workweek in LBP Leasing and Finance Corporation (LLFC).

As a government-owned and controlled corporation (GOCC) under the supervision of Land Bank of the Philippines (LBP) and subject to the oversight of the Governance Commission for GOCCs (GCG), LLFC is mandated to align its operations with applicable government directives while maintaining compliance with Bangko Sentral ng Pilipinas (BSP) regulations, existing Board-approved policies, and the standards required of a financial institution.

SECTION II. LEGAL AND POLICY BASES

This Office Circular is issued pursuant to and in accordance with the following:

1. Office of the President Memorandum Circular No. 114, s. 2026 — Directing All Government Agencies and Instrumentalities to Strictly Adopt Energy Conservation Protocols and Implement a Four-Day Onsite Work Arrangement (PRIMARY BASIS);
2. Civil Service Commission Memorandum Circular No. 06, s. 2022 — Policies on Flexible Work Arrangements in the Government;
3. Republic Act No. 2260, as amended — Civil Service Act;
4. Executive Order No. 292 (Administrative Code of 1987), Book V on Civil Service;
5. Republic Act No. 6713 — Code of Conduct and Ethical Standards for Public Officials and Employees;
6. Republic Act No. 7638 — Department of Energy Act of 1992 and relevant DOE energy conservation circulars;
7. Republic Act No. 10175 — Cybercrime Prevention Act of 2012 (as applicable to data security obligations under WFH arrangement);
8. Republic Act No. 10173 — Data Privacy Act of 2012 and its Implementing Rules and Regulations;
9. Republic Act No. 11032 — Ease of Doing Business and Efficient Government Service Delivery Act of 2018;
10. Republic Act No. 12009 — LBP Leasing and Finance Corporation Charter/Governing Law (as applicable);

11. BSP Circulars on Financial Institution Cybersecurity Standards and Business Continuity Management;
12. GCG Memorandum Circulars on GOCC Operations and Employee Management; and
13. Other applicable laws, rules, and regulations issued by the CSC, DBM, GCG, BSP, COA, DOE, NPC, and other competent government authorities.

SECTION III. OBJECTIVES

This Circular aims to:

1. Implement the Presidential directive on the Four-Day Workweek in a manner consistent with applicable civil service rules and regulations;
2. Establish a skeletal workforce arrangement for Fridays to ensure operational continuity while maximizing the benefits of reduced building occupancy;
3. Prescribe clear and enforceable guidelines for the use of personal devices for WFH, including mandatory ICT security controls to protect LLFC and client data;
4. Ensure the continuity, efficiency, and quality of service delivery to clients, business partners, and government stakeholders of LLFC;
5. Promote employee welfare by providing WFH flexibility while maintaining full accountability for work output and performance;
6. Support the government's austerity and energy conservation program by reducing operational costs, electricity consumption, and fuel use;
7. Rationalize Board and Board-Level Committee meeting schedules in compliance with MC 114 energy conservation objectives;
8. Define the duties and responsibilities of all officers, employees, and units in implementing this policy.

SECTION IV. COVERAGE

A. Covered Personnel

This Circular shall apply to all personnel of LLFC, as follows:

1. Regular/Permanent Employees — All employees with permanent appointments to regular plantilla positions;
2. Contractual/Job Order Workers — As specifically provided in Section IX of this Circular.

B. Exempted Personnel

The following positions/employees may be exempted from the standard WFH Friday arrangement, subject to the approval of the President/CEO:

1. Employees assigned as Skeletal Workforce for the Friday shift, as provided in Section VI-F hereof;
2. Employees whose work requires physical access to LLFC office documents, equipment, or systems not accessible remotely, as identified by the Head of Group/Unit;
3. Employees performing functions that require daily interface with external clients, government agencies, BSP, or the public, and cannot be performed remotely;
4. Employees who have no access to a laptop or reliable internet connection and have elected to report onsite on Fridays under Section VI-G hereof.

SECTION V. GENERAL GUIDELINES

1. The work arrangement under MC 114 shall consist of four (4) days of onsite work (Monday to Thursday) and one (1) common WFH day on Friday. The standard forty (40) hours workweek shall be maintained — employees shall render eight (8) hours of work per day, five (5) days a week.
2. Friday shall be the designated common Work-From-Home (WFH) day for all covered employees who are NOT assigned to the Skeletal Workforce and whose nature of work permits remote performance. LLFC operations shall continue on Fridays through a combination of WFH employees and the Skeletal Workforce present onsite.
3. The implementation shall not result in a reduction of the employee's monthly salary, basic pay, or any existing benefits. Employees shall not suffer diminution of pay as a result of this arrangement.
4. All employees are expected to maintain the same level of productivity, service delivery, and work quality consistent with their Key Result Areas (KRAs) and Individual Performance Commitment and Review (IPCR) under the Strategic Performance Management System (SPMS).
5. Attendance and punctuality shall continue to be strictly monitored and enforced. Daily Time Records (DTR) or biometric/electronic attendance logs shall reflect the actual time in and time out consistent with the prescribed schedule.
6. Overtime work, if required, shall be authorized and compensated in accordance with existing policies on overtime.
7. Employees who are absent on any of the four (4) onsite working days (Monday to Thursday) without approved leave shall be considered Absent Without Official Leave (AWOL) for the day. Failure to render WFH work on Friday — or to report onsite on Friday if assigned to the Skeletal Workforce — without approved leave shall likewise be treated as AWOL.
8. Applicable holidays falling on a Friday (WFH day) shall be treated in accordance with existing rules on regular, special non-working, and special working holidays. An employee who is on WFH on a Friday that is declared a regular holiday shall be entitled to a holiday with pay and shall not be required to render work.
9. The 4DWW shall be implemented as an interim measure pursuant to MC 114, and shall remain in effect until lifted or revoked by the President of the Philippines. Management shall conduct a periodic evaluation of its impact.

SECTION VI. SPECIFIC GUIDELINES

A. Work Schedule

The following work schedule shall apply to all covered employees under the Four-Day Onsite and WFH Friday Arrangement:

	Monday	Tuesday	Wednesday	Thursday	Friday
Mode	ONSITE	ONSITE	ONSITE	ONSITE	**WFH / ONSITE***
Work Hours	8:30 AM – 5:30 PM	8:30 AM – 5:30 PM	8:30 AM – 5:30 PM	8:30 AM – 5:30 PM	8:30 AM – 5:30 PM
Lunch Break	12:00 NN – 1:00 PM No Noon break Cient Facing	12:00 NN – 1:00 PM No Noon break Cient Facing	12:00 NN – 1:00 PM No Noon break Cient Facing	12:00 NN – 1:00 PM No Noon break Cient Facing	12:00 NN – 1:00 PM No Noon break Cient Facing
Total Hours	8 hrs	8 hrs	8 hrs	8 hrs	8 hrs

**Friday arrangement depends on Skeletal Workforce assignment and nature of work. See Sections VI-F and VI-G.*

Note: The standard 8-hour workday (8:30 AM – 5:30 PM) applies on all five days. Alternative start times (e.g., 8:00 AM – 5:00 PM) may be approved by the Head of Group/Unit for WFH Fridays, subject to President's approval, provided the full eight (8) working hours are rendered.

B. Attendance and Time-Keeping

1. All employees shall log their time in and time out using the biometric attendance system or other authorized timekeeping devices on onsite days (Monday to Thursday) and on onsite Fridays.
2. Tardiness of more than fifteen (15) minutes from the prescribed start time shall be recorded and dealt with in accordance with the LLFC Disciplinary Policy.
3. On WFH Fridays, employees shall log their attendance through the Work-From-Home Application System, a designated online attendance platform used by LLFC. Employees shall remain reachable through official communication channels (MS Teams, official email, official mobile number) throughout their prescribed work hours.
4. A WFH Daily Accomplishment Report (DAR) shall be submitted by each WFH employee at the end of every WFH Friday, not later than 5:30 PM, through the Microsoft Teams WFH App, consolidated by the designated personnel per Unit to be signed and approved by the Group/Unit Head.
5. Skeletal Workforce employees reporting onsite on Fridays shall use the biometric attendance system and shall not be required to submit a DAR for that day.

C. Leave Administration

1. Leave credits shall continue to be accrued and administered in accordance with existing CSC Omnibus Rules on Leave.
2. A leave absence of one (1) day under the 4DWW shall be equivalent to eight (8) hours of leave credit deduction, consistent with the standard eight (8)-hour workday under this arrangement.
3. If a regular holiday falls on Friday (WFH day), the employee shall be entitled to a holiday with pay and shall not be required to render WFH work.
4. Employees on maternity leave, paternity leave, parental leave, or other special leaves shall not be affected by the 4DWW for the duration of their approved leave.
5. Leave applications shall be filed at least three (3) working days in advance, except in emergency cases, through the HRIS.

D. Compensation and Benefits

1. No diminution in basic salary, allowances, or other monetary benefits shall result from the implementation of the 4DWW.
2. Skeletal Workforce employees required to report onsite on Fridays shall not receive additional compensation by reason of onsite reporting alone, unless they rendered overtime beyond eight (8) hours that is authorized and as such can be compensated under existing rules.
3. Overtime pay, if authorized, shall be computed on the basis of the hourly rate and applicable premium rates under existing rules.

E. Client Services and Frontline Operations

1. LLFC shall ensure that frontline services, client-facing operations, and regulatory submissions (BSP, COA, BIR, etc.) are not adversely affected by the 4DWW.
2. The Skeletal Workforce on Fridays shall cover all client-facing and critical operational functions that cannot be performed remotely.
3. The LLFC website, and electronic communication channels shall carry a conspicuous notice of the 4DWW schedule and the Friday WFH/skeletal arrangement for the information of clients and the public.
4. For transactions with counterpart agencies or clients requiring coordination on Fridays, the relevant Head of Group/Unit shall ensure that the Skeletal Workforce or designated WFH employees are available and responsive.

F. Skeletal Workforce for Fridays

1. A Skeletal Workforce shall be maintained at the LLFC office every Friday to ensure that essential operations are not disrupted and that critical transactions, client-facing services, and document-dependent processes continue without interruption.
2. Each Head of Group/Unit shall submit to the HRU, within three (3) working days from the effectivity of this Circular, a Skeletal Workforce List for Fridays of March and within five (5) working days before the end of the month for the succeeding month, identifying: (a) the positions/employees required to report onsite every Friday or on a rotating basis; and (b) the specific functions or operational requirements necessitating onsite presence. The list shall be submitted to the President/CEO for approval.
3. The Skeletal Workforce assignment shall be based on objective operational criteria and shall take into account the functions that require physical access to LLFC office documents, systems, equipment, physical vaults, or client reception — functions that cannot be performed remotely without compromising operational integrity or data security.
4. Employees whose work inherently requires physical document processing, originals review, physical filing, client reception, or access to systems, equipment, or records available only onsite shall be designated as part of the Skeletal Workforce for Fridays and shall be required to report to the office on such days.
5. Where operational requirements permit, the Skeletal Workforce assignment may be done on a rotation basis among qualified employees within the group/unit, to distribute the onsite Friday burden equitably. The rotation schedule shall be determined by the Group/Head of Unit and approved by the President/CEO.
6. Skeletal Workforce employees shall be entitled to full compensation for Friday work under the standard schedule. No special premium or incentive shall be paid solely by reason of being assigned to the Skeletal Workforce unless overtime is authorized.
7. The minimum Skeletal Workforce composition per Friday shall be at least one (1) authorized signatory officer or designated officer-in-charge and sufficient support staff to ensure operational coverage. The HRU shall maintain an updated master Skeletal Workforce Schedule.

The following table summarizes the Friday reporting arrangement:

CATEGORY	FRIDAY ARRANGEMENT	BASIS / REQUIREMENT
Skeletal Workforce	REQUIRED ONSITE on Friday	Assigned by Unit Head; approved by President
Document-processing employees	REQUIRED ONSITE on Friday	Nature of work requires physical access to documents, equipment, or systems not accessible remotely

CATEGORY	FRIDAY ARRANGEMENT	BASIS / REQUIREMENT
LLFC laptop issued	WFH on Friday (default)	Must submit WFH Setup Declaration Form and DAR
Personal device (with consent form)	WFH on Friday (with IT security controls)	Personal Device Use Consent and Security Agreement required; full endpoint controls apply
No laptop / no internet	May report ONSITE on Friday	Employee informs HRU/Unit Head; treated as regular onsite WFH-day reporting

G. Employees Without Laptop or Reliable Internet Access

1. Employees who do not have access to a laptop or a reliable internet connection necessary to perform their duties remotely are not required to perform WFH on Fridays.
2. Such employees may opt to report to the LLFC office on Fridays and shall be treated as regular onsite employees for that day. They shall notify their Head of Group/Unit and the HRU of their intention to report onsite on Fridays due to lack of WFH equipment or connectivity.
3. Reporting to the office on Fridays due to lack of WFH capability shall not be treated as a violation of this Circular and shall not be a basis for any adverse action against the employee.
4. The IT Unit shall prioritize the issuance of LLFC-provided laptops to employees who require access to LLFC application systems (including Jeonsoft, NAV, and other core business applications) and who are not assigned to the Skeletal Workforce. The IT Unit shall submit a Laptop Issuance Priority List to the President within three (3) working days from the effectivity of this Circular.
5. Employees who prefer to perform WFH and are not assigned to the Skeletal Workforce, but to whom an LLFC laptop cannot be issued due to the limited number of available laptops, may use their personal devices for WFH subject to full compliance with Section VI-H of this Circular (Personal Device Policy).

H. Personal Device Policy for WFH Friday

Due to the limited number of LLFC-issued laptops and the operational need to extend WFH capability to as many employees as possible, employees who are not assigned to the Skeletal Workforce and to whom no LLFC laptop can be issued may be authorized to use their personal devices (personal laptop, desktop computer, or tablet) for WFH Fridays, subject to the following mandatory conditions:

1. Personal Device Use — Consent Requirement

No employee shall use a personal device for LLFC WFH purposes without first executing a written Personal Device Use Consent and Security Agreement (hereinafter, 'Device Consent') in the form prescribed by the IT Unit. The execution of the Device Consent is a pre-condition to authorization for WFH using a personal device. Use of personal devices without a signed Device Consent shall constitute a policy violation.

2. Mandatory Security Controls on Personal Devices

By executing the Device Consent, the employee gives express and informed consent to the following security measures and obligations, which are mandatory and non-negotiable:

- Multi-Factor Authentication (MFA) — Microsoft Authenticator shall be enforced on the employee's Microsoft 365 (MS365) account. No access to LLFC MS365 applications (Teams, Outlook, SharePoint, OneDrive) shall be granted without MFA enrollment and active MFA verification on each login session. The employee must keep the MFA device secure at all times.
- Endpoint Security Installation — LLFC's prescribed endpoint security software (antivirus/anti-malware/endpoint detection and response solution) shall be installed on the personal device by the IT Unit or as directed by the IT Unit prior to first authorized WFH use, and shall remain installed and active for the entire period during which the personal device is authorized for LLFC WFH. The employee consents to the installation and removal of said endpoint security upon cessation of WFH authorization or upon return to full onsite work.
- VPN for Business Applications — A Virtual Private Network (VPN) client shall be installed on the personal device for accessing LLFC's core business applications, including Jeonsoft and Microsoft Dynamics NAV (NAV). No employee shall access Jeonsoft, NAV, or any LLFC network resource from a personal device without an active, LLFC-approved VPN connection. Attempts to bypass VPN access controls are strictly prohibited.
- Mobile Device Management (MDM) — Upon implementation of LLFC's Mobile Device Management (MDM) solution, personal devices authorized for WFH shall be enrolled in the MDM system. By enrolling in MDM, the employee explicitly consents to the following, limited to the scope of LLFC corporate data and applications:
  a. Enforcement of device security policies (screen lock, encryption, passcode requirements) on the enrolled device as required by LLFC's MDM configuration;
  b. Remote wiping of LLFC corporate data (not personal data) from the personal device in the event of loss, theft, compromise, or upon cessation of WFH authorization;
  c. Restriction of access to sensitive LLFC resources to MDM-compliant devices only;
  d. Monitoring for risky device behavior (including jailbreaking, rooting, malware installation, unauthorized application access) that may compromise LLFC data security;
  e. Automated compliance checks by the MDM system prior to granting access to LLFC resources.
- Reporting of Lost, Stolen, or Compromised Device — An employee whose authorized personal device is lost, stolen, or suspected of being compromised (including unauthorized access, malware infection, or data breach) shall IMMEDIATELY — without delay and not later than one (1) hour after discovery — report the incident to the IT Unit Head and the Head of HRU/Corporate Services Group. The IT Unit shall immediately initiate incident response procedures, including MDM remote wipe of corporate data, revocation of VPN and MS365 credentials, and escalation to Management. The employee shall cooperate fully with any resulting investigation.
- Password and Account Security — The employee shall use a strong, unique password for the personal device (minimum 12 characters, combination of upper/lower case, numbers, and special characters). The LLFC account password shall not be stored in the browser or any unencrypted location on the personal device. The employee shall immediately report to the IT Unit any suspected unauthorized access to their LLFC account.
- Prohibition on Public and Unsecured Networks — The employee shall not access any LLFC system, application, or data using a public Wi-Fi network (e.g., coffee shops, airports, malls, public hotspots). Access shall be restricted to private, secured home networks or a personal mobile data connection. Use of VPN does not authorize access via public Wi-Fi.
- Operating System and Application Security Patching — The personal device's operating system and all installed applications shall be kept up-to-date with the latest security

patches and updates. The IT Unit may prescribe minimum OS version requirements for authorized devices.

- Prohibition on Unauthorized Software and Applications — The employee shall not install applications or software on the personal device that are not necessary for LLFC WFH work and that may pose security risks. Applications with known vulnerabilities, peer-to-peer (P2P) file sharing applications, and unlicensed or cracked software are strictly prohibited.
- Data Minimization and No Local Storage of Confidential Data — Confidential LLFC documents, client data, financial records, and BSP-regulated information shall NOT be downloaded, saved, or stored on the personal device's local storage (hard drive, desktop, documents folder, USB drives). All work shall be done through LLFC's cloud-based platforms (SharePoint, OneDrive for Business) or through the VPN-connected application environment. Printing of confidential LLFC documents at home is strictly prohibited.
- Screen Privacy and Physical Security — The employee shall ensure that their personal device screen cannot be viewed by unauthorized persons (family members, housemates, visitors) while working on LLFC matters. The employee shall use a privacy screen filter if practicable. The personal device shall be kept physically secure at all times.
- IT Unit Right to Audit Compliance — The IT Unit reserves the right to audit, remotely or through self-certification, the compliance of personal devices with the security requirements of this Circular. Employees shall cooperate with such audits and shall not obstruct or disable any installed security software.
- Cessation of Access on Separation or End of WFH Authorization — Upon separation from LLFC, reassignment to full onsite work, or upon revocation of WFH authorization, the employee shall immediately surrender access to all LLFC accounts and systems. The IT Unit shall remotely revoke all access credentials and wipe corporate data from the personal device through MDM. The endpoint security software installed on the personal device shall be removed by the IT Unit.
- Liability for Data Breach — An employee who fails to comply with the Personal Device Policy and whose non-compliance results in unauthorized disclosure, loss, or destruction of LLFC or client data shall be personally liable for the resulting breach, subject to administrative sanctions, civil liability, and potential criminal prosecution under the Cybercrime Prevention Act (RA 10175) and the Data Privacy Act (RA 10173).

3. Scope of IT Unit Assistance — Personal Devices

The IT Unit shall provide initial setup assistance (MFA enrollment, VPN installation, endpoint security installation, MDM enrollment) for authorized personal devices. Ongoing technical support for personal device hardware issues, personal software, or non-LLFC applications is outside the scope of IT Unit responsibility.

I. Board and Board-Level Committee Meeting Schedule Rationalization

In furtherance of the energy conservation and austerity measures mandated by MC 114, and consistent with the objective of reducing non-essential operational activities during the WFH day, the following guidelines shall govern the scheduling of Board of Directors (BOD) and Board-Level Committee meetings:

1. Regular Board of Directors meetings and all Board-Level Committee meetings (including but not limited to the Executive Committee, Audit Committee, Risk Management Committee, Related Party Transaction Committee and Corporate Governance Committee) shall be scheduled on Wednesdays or Thursdays, to the extent practicable.
2. The Corporate Secretary's Office shall observe the Wednesday-or-Thursday scheduling preference in the preparation of all meeting notices, coordination with Board members,

and preparation of board packages, and shall bring this policy to the attention of the Board Chairperson for implementation.

3. Special Board of Directors meetings and Special Board-Level Committee meetings — meetings called outside of the regular schedule due to urgent or exceptional circumstances — are hereby strongly encouraged to be conducted electronically via videoconferencing platforms (Zoom or MS Teams), in lieu of physical convening. Electronic Board and Committee meetings shall be governed by the applicable provisions of the LLFC By-Laws, the Corporation Code of the Philippines (RA 11232, as applicable), the GCG Memorandum Circulars on GOCC governance, and the LLFC Board-approved policies on electronic meetings.
4. The conduct of regular and special meetings via videoconferencing shall comply with quorum requirements, voting procedures, and documentation requirements as prescribed by the Corporation Code, the By-Laws, GCG issuances, and LLFC's Corporate Governance Manual. A complete audio-visual recording and minutes of all electronically-conducted meetings shall be prepared, certified by the Corporate Secretary, and maintained as part of official corporate records.
5. Directors participating in electronic meetings via Zoom or MS Teams from locations other than the LLFC office shall be fully counted for quorum and voting purposes, provided they are identifiable, can participate in real time, and the meeting platform ensures the integrity and security of the proceedings, consistent with applicable law and corporate governance standards.
6. The Corporate Secretary shall include the Wednesday-or-Thursday scheduling policy and the electronic meeting preference in the Annual Corporate Calendar of Board Meetings, which shall be submitted for Board approval at the organizational meeting of the Board at the start of each year.
7. In-person Board and Committee meetings may still be held at the discretion of the Board Chairperson and the President/CEO when the agenda requires physical presence, the signing of original documents, or when electronic means are otherwise impractical. In such cases, the energy conservation measures prescribed in Section VII of this Circular shall be strictly observed during the meeting.

SECTION VII. ENERGY CONSERVATION MEASURES

In strict compliance with Office of the President Memorandum Circular No. 114, s. 2026, all LLFC personnel, units, and facilities shall observe the following energy conservation measures, effective immediately upon the effectivity of this Circular:

A. Electricity Conservation

1. All LLFC offices shall reduce electricity consumption by a minimum of ten (10) percent and shall endeavor to achieve a reduction of up to twenty (20) percent of their average monthly electricity usage, measured against the immediately preceding three-month average;
2. Air-conditioning units in all LLFC offices and common areas shall be set and maintained at twenty-four (24) degrees Celsius at all times during office hours;
3. All non-essential lights, electrical fixtures, and electronic equipment shall be turned off during the one-hour lunch break (12:00 noon to 1:00 PM) and immediately after office hours;
4. All office equipment shall be set to automatic sleep/power-saving mode after a maximum of ten (10) minutes of inactivity;
5. All computers, monitors, and other electrical equipment shall be fully shut down and unplugged at the end of each workday;

6. On WFH Fridays, the reduced onsite population shall result in lower electricity consumption; non-occupied areas shall have all lights and equipment turned off by the Administration Unit;
7. The use of personal electric appliances within office premises is discouraged and subject to approval of the Head of Group/Unit;
8. The IT Unit shall configure all networked devices, servers, and shared equipment to energy-saving settings, consistent with security requirements.

B. Fuel and Transportation Conservation

1. LLFC shall reduce fuel consumption for official vehicles by a minimum of ten (10) percent from average monthly consumption;
2. The use of official vehicles shall be limited to strictly necessary official business and must be pre-approved and documented through a Trip Ticket;
3. Car-pooling among LLFC officers and employees for official business trips is encouraged;
4. Non-essential government travel shall be temporarily suspended pending clearance from the President/CEO;
5. The use of videoconferencing platforms (MS Teams, Zoom) is mandated for all internal and inter-agency meetings that do not require physical presence.

C. Non-Essential Activities — Suspension

Pursuant to MC 114, the following non-essential activities are hereby suspended until further notice:

1. Out-of-town trips for non-essential purposes;
2. In-person team-building activities, recreational events, and social gatherings using office resources;
3. In-person seminars, conferences, and training programs that can be attended virtually;
4. Representation trips and inter-agency courtesy calls that can be conducted via videoconference;
5. Physical convening of meetings — whether internal or with external parties — that can be effectively conducted via MS Teams or Zoom.

D. Monitoring and Reporting

1. A monthly energy consumption report shall be submitted by the Building Administration/General Services unit to the President and CEO, reflecting electricity (kWh) and fuel (liters) consumed versus the baseline and the MC 114 target;
2. A quarterly energy conservation compliance report shall be submitted to the Board of Directors;
3. The IT Unit shall submit a monthly ICT energy savings report to the Head of Corporate Services Group;
4. Non-compliance with energy conservation measures shall be reported to the HRU for appropriate action.

SECTION VIII. CONTRACTUALAND OUTSOURCED PERSONNEL

A. Agency-Hired / Outsourced Personnel

1. Personnel provided by third-party service providers are governed by the Labor Code and the terms of the Service Contract between LLFC and the agency.
2. The Corporate Services Group shall coordinate with respective service agencies to align their deployment schedules with the LLFC 4DWW schedule.

3. Adjustments in Friday deployment shall be negotiated with service providers and documented through formal contract amendments, subject to COA and BAC approval if necessary.

SECTION IX. DUTIES AND RESPONSIBILITIES

A. President and CEO

1. Issue the specific effectivity date and supplemental memoranda necessary for the implementation of this Circular;
2. Approve the Skeletal Workforce List submitted by each Head of Unit;
3. Approve requests for exemption from the 4DWW schedule based on operational necessity;
4. Approve the IT Unit's Laptop Issuance Priority List;
5. Ensure that the Board of Directors is kept informed of the status of 4DWW implementation and its impact on operations and employee welfare;
6. Submit required reports to GCG, CSC, and other oversight bodies as may be required.

B. Head of Corporate Services Group / Human Resource Unit

1. Prepare, disseminate, and monitor compliance with this Circular and all supplemental issuances;
2. Collect and maintain WFH Setup Declaration Forms, Personal Device Use Consent and Security Agreements, and Skeletal Workforce Lists from all units;
3. Maintain and update the master list of: (a) covered and exempted employees; (b) Skeletal Workforce assignments; (c) employees on LLFC-issued laptops; (d) employees authorized to use personal devices;
4. Oversee timekeeping, attendance monitoring, and DTR processing under the new schedule;
5. Process and evaluate leave applications, overtime requests, and other personnel actions affected by the 4DWW;
6. Conduct an orientation and briefing for all employees within ten (10) working days from effectivity of this Circular;
7. Review and revise all existing JO/COS contracts to conform with the 4DWW schedule;
8. Submit a quarterly implementation report to the President and CEO, with findings, challenges, and recommendations;
9. Record energy conservation violations in the employee's 201 file where warranted;
10. Act as the primary liaison with the CSC, GCG, and DBM on matters related to the Four-Day Onsite and WFH Friday Arrangement.

C. Heads of Groups/ Units Heads

1. Ensure full compliance of their respective unit's employees with this Circular;
2. Prepare and submit the Skeletal Workforce List for Fridays within ten (10) working days from effectivity;
3. Identify employees requiring LLFC laptop issuance and endorse the same to the IT Unit with justification;
4. Identify employees who have no laptop or internet access and coordinate their onsite Friday reporting with the HRU;

5. Ensure that client-facing services and regulatory obligations are continuously met under the 4DWW;
6. Monitor attendance, punctuality, and productivity of their staff and report any violations to the HRU;
7. Review and approve WFH DARs submitted by their subordinates every Friday;
8. Endorse any request for Friday work or skeletal workforce adjustment to the President and CEO with supporting justification.

D. Accounting Unit

1. Ensure that payroll processing, disbursement of salaries and benefits, and financial reporting deadlines are not disrupted by the 4DWW;
2. Coordinate with the HRU on the computation of overtime pay and other compensation adjustments arising from the 4DWW;
3. Process contract amendments with third-party service providers that may result in changes in service fees;
4. Monitor and report cost savings achieved as a result of the 4DWW for submission to Management and the Board.

E. IT Unit

1. Submit the Laptop Issuance Priority List to the President/CEO within ten (10) working days from effectivity, prioritizing employees who require access to LLFC application systems (Jeonsoft, NAV, and other core systems) and who are not assigned to the Skeletal Workforce;
2. Prepare the Personal Device Use Consent and Security Agreement form and ensure its execution by all employees authorized to use personal devices for WFH;
3. Install, configure, and verify endpoint security software, VPN client, and MFA on all authorized personal devices prior to first WFH use;
4. Enroll authorized personal devices in the MDM system upon its deployment and maintain MDM compliance monitoring;
5. Configure all LLFC-issued laptops and personal devices with mandatory power-saving settings, screen lock policies, and auto-logout after prescribed inactivity periods;
6. Maintain a registry of all devices (LLFC-issued and personal) authorized for WFH, including device type, OS version, MFA enrollment status, VPN status, endpoint security status, and MDM enrollment status;
7. Conduct periodic (at minimum quarterly) audits of WFH device security compliance and submit an IT Security Compliance Report to the Head of Corporate Services Group;
8. Immediately revoke access and initiate remote wipe procedures upon receiving a report of a lost, stolen, or compromised device, within one (1) hour of notification;
9. Ensure functionality and security of the HRIS attendance platform, VPN, MS Teams, SharePoint, and all systems required for WFH Friday operations;
10. Issue and enforce comprehensive WFH Data Security and ICT Use Protocols as a supplemental issuance to this Circular, consistent with BSP cybersecurity standards and the Data Privacy Act;
11. Remove all LLFC endpoint security software from personal devices upon cessation of WFH authorization, separation, or full return to onsite work;
12. Configure all networked devices, servers, and workstations to energy-saving settings consistent with security requirements;

13. Ensure that videoconferencing infrastructure (Zoom, MS Teams) is fully functional to support the mandatory shift to virtual meetings;
14. Provide technical support for the Skeletal Workforce and WFH employees on Fridays through a designated IT duty officer or on-call arrangement.

F. Corporate Secretary/BOD Level Committee Secretariat

1. Observe the Wednesday-or-Thursday scheduling preference for all regular Board of Directors and Board-Level Committee meetings;
2. Coordinate with the Board Chairperson, Board members, and the President/CEO to implement the meeting rationalization policy under Section VI-I of this Circular;
3. Facilitate the conduct of Special BOD and Special Committee meetings via Zoom or MS Teams, ensuring compliance with quorum, voting, documentation, and recording requirements;
4. Include the Board meeting schedule rationalization policy in the Annual Corporate Calendar of Board Meetings;
5. Ensure that minutes and recordings of all electronically-conducted Board and Committee meetings are properly certified and archived.

G. All Employees

1. Comply strictly with the prescribed 4DWW schedule, Skeletal Workforce assignment (if applicable), and all provisions of this Circular;
2. Execute the WFH Setup Declaration Form and, if using a personal device, the Personal Device Use Consent and Security Agreement, before the first WFH Friday;
3. Comply with all ICT security requirements for personal devices as prescribed in Section VI-H of this Circular;
4. Immediately report to the IT Unit any lost, stolen, or compromised personal device authorized for WFH use;
5. Submit the WFH Daily Accomplishment Report (DAR) to their immediate supervisor by 5:30 PM every WFH Friday;
6. Refrain from downloading, storing, or printing confidential LLFC or client documents on personal devices or home printers;
7. Maintain a suitable, safe, and secure home work environment on WFH Fridays;
8. Comply with all energy conservation measures prescribed in Section VII of this Circular;
9. Report any concerns, difficulties, or violations related to the implementation of the 4DWW to their respective Head of Unit or the HRU.

SECTION X. VIOLATIONS AND SANCTIONS

Non-compliance with the provisions of this Circular shall be dealt with administratively in accordance with the LLFC Disciplinary Policy and other applicable rules. All disciplinary actions shall be conducted with full observance of due process rights, including the right to be informed of the charges and the right to be heard, consistent with LLFC's Office Circular on Disciplinary Procedures.

SECTION XI. MONITORING, EVALUATION, AND REPORTING

1. The HRU, in coordination with all Heads of Groups/Units, shall conduct a monthly assessment of the 4DWW implementation, covering attendance compliance, Skeletal Workforce adequacy, productivity indicators, WFH device compliance, cost savings, and client service delivery quality.
2. A Preliminary Evaluation Report shall be submitted to the President and CEO within sixty (60) days from the effectivity of the 4DWW.
3. A Comprehensive Six-Month Review Report shall be submitted to the President/CEO upon completion of the pilot period, with recommendations for continuation, modification, or discontinuation.
4. The IT Unit shall submit a quarterly ICT Security and WFH Device Compliance Report to the Head of Corporate Services Group.
5. LLFC shall submit any mandatory reports required by the oversight bodies in connection with the 4DWW and MC 114 implementation, as needed.

SECTION XII. TRANSITORY PROVISIONS

1. During the transition period (first thirty (30) calendar days from effectivity), the HRU shall provide liberal guidance to employees adjusting to the new schedule.
2. The IT Unit shall have ten (10) working days from effectivity to complete MFA enrollment, VPN installation, endpoint security installation, and MDM enrollment for all WFH-authorized personal devices. During this period, WFH using personal devices shall not commence until the IT Unit certifies the device as compliant.
3. Existing work arrangements, flexi-time agreements, and special schedules shall remain effective until reviewed and adjusted by the HRU in accordance with this Circular.
4. The HRU shall coordinate with the Accounting Unit to ensure seamless transition in payroll processing and timekeeping during the first full payroll cycle under the 4DWW.

SECTION XIII. MISCELLANEOUS PROVISIONS

1. Separability Clause. If any provision of this Circular is found inconsistent with a subsequent issuance of the CSC, GCG, BSP, or other competent authority, such provision shall be deemed modified accordingly, but the rest of the Circular shall remain in full force and effect.
2. Amendment. This Circular may be amended, supplemented, or revoked as may be warranted by operational requirements, regulatory directives, or evaluation results, subject to President/CEO approval.
3. Supplemental Issuances. The IT Unit shall issue the WFH Data Security and ICT Use Protocols as a supplemental issuance within ten (10) working days from effectivity. The HRU may issue supplemental FAQs or advisories to clarify the application of this Circular to specific situations. Likewise, Administrative Unit may issue separate Circular for Energy Conservation measures.
4. Effectivity. This Circular shall take effect upon approval and shall remain in effect until revoked or modified.

SECTION XIV. DISSEMINATION AND ACKNOWLEDGMENT

All Heads of Groups/Units are directed to ensure that this Circular is promptly disseminated to all employees under their supervision. Each employee shall sign an Acknowledgment Receipt confirming that they have read and understood the provisions of this Circular. The HRU shall maintain a master file of all signed acknowledgment receipts.

For strict compliance.

[redacted]

ROBERTO U. TEO
President and CEO

Date: March 9, 2026

The following Annexes shall be an integral part of this Office Circular 26-002:

- Annex A – Acknowledgment Receipt
- Annex B - Personal Device Use Consent and Security Agreement

ANNEX "A"

ACKNOWLEDGMENT RECEIPT

Office Circular No. 2026-002 Series 2026
Four-Day Onsite Work, WFH Friday with Skeletal Workforce, Personal Device Policy, and Energy Conservation Pursuant to Office of the President Memorandum Circular No. 114, s. 2026

I hereby acknowledge receipt of a copy of Office Circular No. 02-2026. I confirm that I have read and understood its provisions — including the Skeletal Workforce assignment policy, Personal Device Use Policy and ICT security requirements, WFH Friday guidelines, Board meeting schedule rationalization, and Energy Conservation Measures — and I agree to comply with all applicable guidelines.

Name and Signature	Date Received/ Signed:	
Position and Designation	WFH Device:	[_] LLFC Laptop [_] Personal Device
Group/Unit	Others:	[_] No WFH/ Onsite Friday

For HRU Use Only

Date filed in 201 File: _____

Personal Device Consent on file: [ ] YES [ ] N/A

Filed by: _____

ANNEX "B"

PERSONAL DEVICE USE CONSENT AND SECURITY AGREEMENT

PURPOSE: This Personal Device Use Consent and Security Agreement ('Agreement') is executed by the undersigned employee of LBP Leasing and Finance Corporation ('LLFC') in connection with the use of a personal device (laptop, desktop computer, or tablet) for Work-From-Home ('WFH') purposes on designated WFH Fridays, pursuant to **Office Circular No. 2026-002 on the Four-Day Onsite Work and WFH Friday Arrangement** and **Office of the President Memorandum Circular No. 114, s. 2026**. Execution of this Agreement is a mandatory pre-condition to authorization for WFH using a personal device. This Agreement constitutes a legally binding undertaking.

PART A. PERSONAL DEVICE INFORMATION

PERSONAL DEVICE INFORMATION SHEET	
Device Type	☐ Laptop ☐ Desktop ☐ Tablet
Brand / Model	
Serial Number	
Operating System	☐ Windows 10 ☐ Windows 11 ☐ macOS ☐ Other: _____
OS Version	
LLFC MS365 Email	
Employee No.	
IT Setup Date	
IT Setup Performed by	

PART B. EMPLOYEE DECLARATIONS AND EXPRESS CONSENTS

I, the undersigned employee, hereby DECLARE and CONFIRM the following, and hereby give my **EXPRESS, INFORMED, AND VOLUNTARY CONSENT** to the installation and enforcement of the security measures and obligations described below on my personal device, as a condition of my authorization to use said personal device for LLFC WFH purposes:

B.1 Multi-Factor Authentication (MFA) — Microsoft Authenticator

- I consent to the mandatory enrollment of my LLFC Microsoft 365 (MS365) account in Multi-Factor Authentication (MFA) using the Microsoft Authenticator application.

B.1 Multi-Factor Authentication (MFA) — Microsoft Authenticator

- I understand that no access to LLFC MS365 applications — including but not limited to Microsoft Teams, Outlook, SharePoint, and OneDrive for Business — shall be granted to my account from any device without successful MFA verification on each login session.
- I commit to keeping my MFA-enrolled device (mobile phone or authenticator device) secure, and to reporting immediately to the IT Unit any loss, theft, or compromise of my MFA device.
- I shall not share my MFA codes, one-time passwords (OTPs), or authentication prompts with any other person under any circumstances.

B.2 Endpoint Security Software — Installation and Removal

- I consent to the installation of LLFC's prescribed endpoint security software (which may include antivirus, anti-malware, and/or endpoint detection and response solution) on my personal device by the LLFC IT Unit or as directed by the IT Unit, as a pre-condition to the first authorized WFH use.
- I understand and agree that the endpoint security software shall remain installed and active on my personal device for the entire period during which my personal device is authorized for LLFC WFH use.
- I consent to the removal of the endpoint security software from my personal device by the LLFC IT Unit upon: (a) cessation of my WFH authorization; (b) my separation from LLFC; or (c) my full return to onsite work, whichever occurs first.
- I shall not disable, uninstall, tamper with, or circumvent the endpoint security software at any time during the authorization period.
- I understand that tampering with or disabling the endpoint security software shall constitute a violation of this Agreement and may result in immediate revocation of my WFH privilege and administrative sanctions.

B.3 Virtual Private Network (VPN) — Access to LLFC Business Applications

- I consent to the installation of an LLFC-prescribed VPN client on my personal device for the purpose of accessing LLFC's core business applications, including Jeonsoft and Microsoft Dynamics NAV (NAV).
- I understand and agree that I shall NOT access Jeonsoft, NAV, or any LLFC internal network resource from my personal device without an active, LLFC-approved VPN connection.
- I shall not share my VPN credentials with any other person.
- I shall not attempt to bypass VPN access controls or access LLFC systems through unauthorized means. Circumvention of VPN requirements is strictly prohibited and shall be treated as a serious disciplinary infraction.
- I shall immediately report to the IT Unit any VPN connectivity issues or suspected unauthorized use of my VPN credentials.

B.4 Mobile Device Management (MDM) — Enrollment and Corporate Data Controls

- I understand that upon implementation of LLFC's Mobile Device Management (MDM) solution, my personal device shall be enrolled in the MDM system as a condition of continued WFH authorization.

B.4 Mobile Device Management (MDM) — Enrollment and Corporate Data Controls

▸ By executing this Agreement, I give my EXPRESS CONSENT to the following MDM actions, LIMITED IN SCOPE to LLFC corporate data and corporate applications on my personal device only:

a. Enforcement of device security policies — The MDM system shall enforce security configurations on my personal device, including but not limited to: screen lock requirements, minimum passcode/PIN length, and full-disk encryption (e.g., BitLocker for Windows or FileVault for macOS). I understand these configurations are applied only as technically necessary to protect LLFC corporate data.

b. Remote wiping of LLFC corporate data — In the event of loss, theft, or compromise of my personal device, or upon cessation of my WFH authorization or separation from LLFC, the IT Unit may remotely wipe LLFC corporate data (including corporate emails, documents, and application data) from my personal device. I understand that remote wipe shall be targeted to corporate data and corporate containers only and shall NOT delete my personal files, personal photos, personal applications, or personal data outside of LLFC corporate containers, to the extent technically feasible by the MDM solution in use.

c. Restriction of access to sensitive LLFC resources — The MDM system may restrict my access to LLFC resources (emails, SharePoint, OneDrive) to MDM-enrolled and MDM-compliant devices only. If my device falls out of compliance with MDM policies, access may be automatically suspended until compliance is restored.

d. Monitoring for risky device behavior — The MDM system may monitor my enrolled personal device for behaviors that pose a security risk to LLFC corporate data, including: device jailbreaking or rooting, installation of applications flagged as malicious, outdated OS or application versions below LLFC minimum requirements, and unauthorized modifications to security configurations. I understand that such monitoring is limited to device compliance status and risk signals, and does not constitute monitoring of my personal activities, personal communications, or personal files.

e. Automated compliance checks — The MDM system shall conduct automated compliance checks prior to granting my device access to LLFC resources.

B.5 Reporting of Lost, Stolen, or Compromised Personal Device

▸ I understand that the immediate reporting of a lost, stolen, or compromised personal device is a critical security obligation under this Agreement and under LLFC Office Circular No. 2026-002.

▸ In the event that my authorized personal device is: (a) lost; (b) stolen; (c) accessed without my authorization; (d) infected with malware; or (e) otherwise suspected of being compromised in any manner that may affect LLFC data security, I hereby commit to reporting the incident IMMEDIATELY — and in no case later than ONE (1) HOUR after discovery — to:

▸ ▸ IT Unit Head: _____ Contact: _____

▸ ▸ Head of Corporate Services Group / HRU: Contact: _____

▸ Upon such report, I agree to cooperate fully with the IT Unit's incident response procedures, including but not limited to: (a) MDM remote wipe of LLFC corporate data; (b) revocation of my VPN and MS365 credentials; (c) surrender of the device for forensic inspection if required; and (d) participation in any administrative investigation arising from the incident.

B.5 Reporting of Lost, Stolen, or Compromised Personal Device

- I acknowledge that failure to report a lost, stolen, or compromised device within the prescribed time frame may result in disciplinary action and personal liability for any resulting data breach.

B.6 Password, Account Security, and Authentication

- I commit to using a strong, unique password for my personal device: minimum twelve (12) characters, combining uppercase and lowercase letters, numbers, and special characters.
- I shall NOT store my LLFC account password in any web browser's auto-fill/password manager, unencrypted file, sticky note, or any insecure location on my personal device.
- I shall NOT share my LLFC account credentials, VPN credentials, or MFA codes with any other person, including family members, colleagues, or IT personnel. LLFC IT staff will never ask for my password.
- I shall immediately report to the IT Unit any suspected unauthorized access to my LLFC accounts.
- I shall change my LLFC account password immediately upon any known or suspected compromise.

B.7 Network Security — Prohibition on Public and Unsecured Networks

- I understand and agree that I shall NOT access any LLFC system, application, or data from any public Wi-Fi network, including but not limited to: coffee shops, restaurants, airports, shopping malls, hotels, and any publicly accessible hotspot.
- WFH access shall be restricted to my private, password-protected home network or my personal mobile data connection (mobile broadband/LTE/5G).
- I understand that VPN connection does NOT authorize use of public Wi-Fi for LLFC access. The prohibition on public Wi-Fi applies regardless of whether VPN is active.
- If I use mobile data (SIM-based internet), I shall ensure that my mobile hotspot is password-protected and not shared with unauthorized users.
- I shall report to the IT Unit any suspected unauthorized access to my home network that may affect LLFC data.

B.8 Operating System and Software Security Maintenance

- I commit to keeping my personal device's operating system and all installed applications updated with the latest official security patches and updates at all times during my WFH authorization period.
- I understand that the IT Unit may prescribe minimum operating system version requirements for authorized devices and that failure to maintain the minimum version may result in suspension of my WFH access until compliance is restored.
- I commit to enabling automatic updates on my personal device for the operating system and for the LLFC-installed security software.
- I shall NOT install applications or software obtained from unofficial sources, including cracked, pirated, or unlicensed applications.
- I shall NOT install peer-to-peer (P2P) file-sharing applications (e.g., BitTorrent clients) on any personal device authorized for LLFC WFH use.

B.8 Operating System and Software Security Maintenance

- I shall NOT install applications with known security vulnerabilities or those flagged by LLFC IT as prohibited applications.

B.9 Data Protection — No Local Storage of LLFC Confidential Data

- I understand that LLFC confidential documents, client data, financial records, credit information, BSP-regulated information, and all other non-public LLFC data shall NOT be downloaded, saved, copied, or stored on my personal device's local storage — including the hard drive, desktop, Documents folder, Downloads folder, external USB drives, personal cloud storage accounts (e.g., personal Google Drive, personal Dropbox, personal iCloud), or any other personal storage medium.
- All WFH tasks involving LLFC data shall be performed through LLFC's authorized cloud platforms — specifically SharePoint, OneDrive for Business (corporate account), and through the VPN-connected application environment (Jeonsoft, NAV).
- I shall NOT print any LLFC confidential document from my personal printer at home. Physical printing of LLFC documents during WFH is strictly prohibited.
- I shall NOT take photographs or screen captures of confidential LLFC data, client information, or internal LLFC documents and store them in personal galleries, albums, or files.
- Upon revocation of my WFH authorization or upon separation from LLFC, I shall immediately delete any LLFC-related files that may have been inadvertently saved to my personal device and confirm deletion to the IT Unit.

B.10 Physical Security and Screen Privacy

- I commit to ensuring that my personal device screen is not visible to unauthorized persons — including family members, housemates, domestic helpers, or visitors — while I am working on LLFC matters.
- I shall use a dedicated, private workspace at my WFH location to the extent practicable, and shall lock or turn off my screen when leaving my workstation, even briefly.
- My personal device shall be physically secured at all times while it contains active LLFC sessions or data — including secure storage when not in use and prevention of unauthorized access by others in my household.
- I shall enable automatic screen lock after no more than five (5) minutes of inactivity and shall require password/PIN/biometric authentication to unlock.
- The use of privacy screen filters is strongly encouraged when working in any location where screen visibility to others cannot be fully controlled.

B.11 Cooperation with IT Security Audits and Inspections

- I acknowledge that the LLFC IT Unit reserves the right to conduct periodic audits of security compliance for authorized personal devices, which may include: remote compliance checks through the MDM system; self-certification forms to be completed by the employee; physical inspection of the device upon request; and log reviews of LLFC application access.
- I commit to cooperating fully and promptly with any such audit or inspection and to providing accurate and complete information regarding the security configuration of my personal device.

B.11 Cooperation with IT Security Audits and Inspections

- I shall NOT disable, tamper with, or obstruct any installed LLFC security software or MDM configuration during or outside of audit periods.
- I acknowledge that failure to cooperate with a security audit may result in the immediate suspension of my WFH privilege pending resolution.

B.12 Cessation of Access — Separation or End of WFH Authorization

- I understand and agree that upon the occurrence of any of the following events — (a) my resignation, retirement, or termination from LLFC; (b) revocation of my WFH authorization by Management; or (c) full return to onsite work — I shall:
  - Immediately cease accessing all LLFC systems and accounts from my personal device;
  - Submit my personal device to the IT Unit for decommissioning of LLFC security software within three (3) working days;
  - Confirm in writing to the IT Unit that no LLFC data remains stored on my personal device;
  - Return any LLFC-specific hardware or tokens (if any) issued in connection with WFH setup.
- I consent to the IT Unit remotely revoking all access credentials, remotely wiping corporate data through MDM, and removing endpoint security software upon the occurrence of the above events.
- I understand that my obligation of confidentiality regarding LLFC data accessed during the WFH period survives the cessation of my WFH authorization and my separation from LLFC.

PART C. SPECIFIC PROHIBITIONS — PERSONAL DEVICE DURING WFH

The following are expressly PROHIBITED while my personal device is authorized for LLFC WFH use:

- Accessing LLFC systems without VPN when VPN is required;
- Accessing LLFC systems through any public or shared Wi-Fi network;
- Sharing LLFC login credentials, VPN credentials, or MFA codes with any person;
- Disabling, uninstalling, or circumventing LLFC endpoint security software or MDM configuration;
- Downloading or locally saving LLFC confidential data, client records, or financial documents on the personal device;
- Printing LLFC confidential documents from a home printer;
- Photographing or screen-capturing confidential LLFC data for personal storage;
- Installing unlicensed, pirated, or P2P file-sharing software on the authorized personal device;
- Allowing unauthorized persons to use the personal device while an LLFC session is active;
- Storing LLFC confidential data in personal cloud storage accounts (personal Google Drive, Dropbox, iCloud, etc.);
- Using AI chatbots, generative AI tools, or other external online platforms to process, upload, or analyze LLFC confidential data;
- Delaying the reporting of a lost, stolen, or compromised device beyond one (1) hour from discovery;

- Obstructing or failing to cooperate with IT security audits;
- Accessing LLFC systems from a jailbroken or rooted personal device.

PART D. ACKNOWLEDGMENT OF LLFC'S RIGHTS AND REMEDIES

I expressly acknowledge the following rights of LLFC in connection with this Agreement:

1. LLFC retains full ownership of all data, documents, records, and intellectual property created or accessed in connection with LLFC business, regardless of which device was used and regardless of the device's storage location.
2. LLFC has the right to immediately revoke my WFH authorization and my access to all LLFC systems in the event of a breach of this Agreement, a security incident, or upon reasonable suspicion of unauthorized data access.
3. LLFC has the right to conduct forensic investigation of my personal device in the event of a data security incident, subject to applicable laws, with my express cooperation.
4. Breach of this Agreement may result in: (a) administrative sanctions up to and including dismissal from service; (b) civil liability for any loss, damage, or compromise suffered by LLFC or its clients as a result of my non-compliance; and (c) criminal prosecution under applicable laws, including the Cybercrime Prevention Act of 2012 (RA 10175) and the Data Privacy Act of 2012 (RA 10173).
5. LLFC's installation of endpoint security and MDM tools on my personal device does NOT give LLFC access to my personal files, personal communications, or personal accounts, and LLFC shall exercise its remote capabilities only to the extent necessary to protect corporate data and as described in this Agreement.

PART E. EMPLOYEE CERTIFICATION CHECKLIST

By initialing each item below, I confirm that I have read, understood, and voluntarily agreed to each of the following:

INITIAL	CONSENT ITEM
_____	I consent to MFA enrollment on my MS365 account (B.1);
_____	I consent to installation and removal of endpoint security software on my personal device (B.2);
_____	I consent to VPN installation and mandatory VPN use for Jeonsoft and NAV access (B.3);
_____	I consent to MDM enrollment and the associated corporate data controls, including remote wipe of LLFC corporate data (B.4);
_____	I understand my obligation to report a lost/stolen/compromised device within one (1) hour (B.5);
_____	I commit to password and account security practices prescribed in this Agreement (B.6);
_____	I commit to accessing LLFC systems only through secured private networks, not public Wi-Fi (B.7);
_____	I commit to keeping my personal device's OS and applications fully patched and updated (B.8);

INITIAL	CONSENT ITEM
_____	I commit to NOT downloading, saving, or storing LLFC confidential data on my personal device (B.9);
_____	I commit to physical device security and screen privacy practices (B.10);
_____	I consent to IT security audits and commit to full cooperation (B.11);
_____	I understand my obligations upon cessation of WFH authorization, including device decommissioning (B.12);
_____	I understand the specific prohibitions in Part C and commit to observing all of them;
_____	I acknowledge LLFC's rights and remedies under Part D, including potential criminal liability for data breaches.

PART F. DECLARATION AND EXECUTION

IN WITNESS WHEREOF, I hereby execute this Personal Device Use Consent and Security Agreement freely and voluntarily, with full knowledge of its contents and legal consequences, on the date written below. I confirm that I was not coerced, deceived, or unduly pressured into executing this Agreement and that I have had sufficient opportunity to seek clarification from the LLFC IT Unit and Human Resource Unit before signing.

Employee Signature over Printed Name:

_____

Position / Designation:

_____

Group / Unit:

_____

Date Executed:

_____

Received and Witnessed by:

_____

IT Unit Head / Authorized IT Personnel

Date Received by IT Unit:

_____

Noted by:

_____

Head of Corporate Services Group / HRU

PART G. IT UNIT SETUP AND SECURITY CERTIFICATION

TO BE COMPLETED BY THE IT UNIT. This certification confirms that the personal device described in Part A has been configured with the required LLFC security controls prior to the employee's first WFH use.

	SECURITY CONTROL	STATUS	REMARKS
1	MFA / Microsoft Authenticator enrolled on MS365 account	☐ Done ☐ N/A	
2	Endpoint security software installed and active	☐ Done ☐ N/A	
3	VPN client installed and tested (Jeonsoft / NAV access)	☐ Done ☐ N/A	
4	MDM enrollment completed (if MDM system is live)	☐ Done ☐ N/A	
5	OS version verified as compliant with IT minimum requirement	☐ Done ☐ N/A	
6	Auto screen lock enabled (max 5 minutes)	☐ Done ☐ N/A	
7	Full-disk encryption confirmed (BitLocker/FileVault)	☐ Done ☐ N/A	
8	Personal device registered in LLFC IT device registry	☐ Done ☐ N/A	
9	Employee provided with WFH Data Security Protocols	☐ Done ☐ N/A	
10	Employee briefed on Incident Reporting Procedure	☐ Done ☐ N/A	

IT Unit Certifying Officer:

_____

Signature over Printed Name

Designation:

_____

Date of IT Certification:

_____

IT Assessment Result:

☐ **DEVICE APPROVED FOR WFH USE**

☐ DEVICE NOT YET APPROVED — Pending: _____

FOR HRU USE ONLY Date received by HRU: _____ 201 File Updated: ☐ Yes ☐ No Received by: _____

This Agreement shall be retained in the employee's 201 File and a copy provided to the IT Unit.