GOVERNMENT OF KERALAM

No.70/2026/Fin Thiruvananthapuram, Dated,18/11/2026

Finance (ITSF) Department

CIRCULAR

Sub: Standard Operating Procedure (SOP) for establishing connectivity between SPARK and other software applications of Government Departments/ Agencies — Modified Guidelines — Issued — reg.

Ref: Circular No. 83/2018/Fin dated 07/09/2018.

As per the circular read above, the established Standard Operating Procedure (SOP) to be adhered to by a Government Department/Agency, State or Central, that formally raised the matter with SPARK PMU for application-to-application (A2A) integration, data sharing and interoperability of their software applications with SPARK in an effective and secured manner, has already been put in place.

2] In view of the escalating volume of data, complexity of organisational data, confidentiality of information maintained and facilitated through SPARK, particularly personal and employee-related data, Government is inclined to the firm view that the SOP for establishing connectivity and structured data exchange has to be reinforced by incorporating additional safeguards encompassing data privacy and protection, information asset classification, access control and privilege administration, authorised use of data utilisation and processing protocols, secure data storage and retention, controlled information sharing, secure data transfer and inter-system exchange protocols, and for institutional accountability, traceability, compliance oversight and audit trail management.

3] Accordingly, Government hereby stipulates that the following documents shall henceforth form part of the SOP:

1. Annexure A – Data Transfer/Connectivity Request and Authorization Format
2. Annexure B – Non-Disclosure Agreement (NDA)
3. Annexure C – Confidentiality Undertaking Format

4] Adequate and comprehensive safeguards are intended to substantially minimize and not just mitigate the possibilities of unauthorized - access, extraction, replication, reproduction, dissemination or misappropriation of data by the requisitioning Department/Agency and to ensure that data transfer is carried out through a clear and standardized process.

5] In order to ensure the operationalization of the aforementioned data protection, information security and confidentiality measures, Government hereby authorise the Chief Project Manager, SPARK PMU to execute the Non-Disclosure Agreement (NDA) on behalf of SPARK PMU, Finance Department, Government of Kerala.

6] All Government Departments/Agencies formally communicating with Finance (SPARK PMU) Department or Finance (ITSF) Department on the matter of establishing connectivity between SPARK and the respective software applications developed, deployed or maintained by those Departments/Agencies shall strictly comply with the aforesaid guidelines and the prescribed SOP, including the requirements contained in Annexures A, B and C.

7] In the event of any breach or contravention from the aforementioned guidelines and instructions, the Heads of Departments should take prompt preventive measures and consequential disciplinary actions and shall report the same to Finance (ITSF) Department mandatorily and expeditiously.

SURESH KUMAR O B
ADDITIONAL SECRETARY

To:

1. The Accountant General (A&E/Audit-II), Kerala, Thiruvananthapuram.
2. The Chief Secretary, All Additional Chief Secretaries/Principal Secretaries /Secretaries/ Special Secretaries/Additional Secretaries/Joint Secretaries/Deputy Secretaries/Under Secretaries to Government.
3. All Heads of Departments/Offices (Through e-office notice board).
4. All Departments and Sections of the Secretariat including Law (Through e-office notice board)
5. The Director of Treasuries, Thiruvananthapuram.
6. The Nodal Officer, www.finance.kerala.gov.in.
7. The Chief Project Manager, SPARK.
8. The Director, Kerala State IT Mission
9. The Stock File/Office Copy (SPK-A2/136/2018-Fin /937530)

Forwarded / By order,

Manager, ITSF

SERVICE AND PAYROLL ADMINISTRATIVE REPOSITORY FOR KERALA (SPARK)
FINANCE (SPARK PMU) DEPARTMENT
GOVERNMENT OF KERALA

STANDARD OPERATING PROCEDURE (SOP)
FOR ESTABLISHING CONNECTIVITY BETWEEN SPARK AND OTHER SOFTWARE APPLICATIONS
OF GOVERNMENT DEPARTMENTS/AGENCIES

SOP VERSION HISTORY

VERSION NO.	PREPARED BY	APPROVED BY	APPROVED DATE	REMARKS
1	Manager, SPARK	Principal Secretary, Finance	01.09.2018	
2	Project Manager, SPARK	Chief Project Manager, SPARK	19-11-2026	

SPARK Project Management Unit
University of Kerala Office Campus, Palayam, Thiruvananthapuram

I. PURPOSE OF THIS SOP

SPARK is the principal Employee Management Information System of Government of Kerala. It necessitates connectivity between SPARK and many other software applications of various departments of Government to share services and data. This Standard Operating Procedure (SOP) establishes a uniform, secure, and auditable process for sharing digital data — within the department, with other government entities, and with agencies— to ensure confidentiality, integrity, and legal compliance in all data-sharing activities.

II. SCOPE OF THIS SOP

Scope of this SOP is to facilitate systematic, scientific and secured sharing of services and data between SPARK and other software applications of various departments under Government of Kerala and Government of India.

III. EXPANSIONS/EXPLANATIONS TO THE TERMS USED IN THIS SOP

a. **SPARK** would mean Service and Payroll Administrative Repository for Kerala
b. **PMU** would mean SPARK Project Management Unit
c. **Applicant Department/Agency**: Government department/ agency, state or central, that approaches SPARK PMU for connecting their software applications with SPARK for data sharing.
d. **Connectivity** would mean connectivity to share services and data between SPARK and other software applications.
e. **SPARK Developer** would mean the SPARK Development Team of NIC, Kerala at its Headquarters.

IV. PROCEDURES TO BE FOLLOWED BY THE APPLICANT DEPARTMENT/AGENCY

a. The applicant department/agency shall submit ANNEXURE A – APPLICATION FORM, ANNEXURE B – Non-Disclosure Agreement (NDA), ANNEXURE C – Confidentiality Undertaking Format (duly signed by the Head of the Department/Agency) to the SPARK Project Management Unit, Finance Department.
b. The applicant department/agency shall furnish further clarifications if any sought by SPARK PMU on time.
c. The applicant department/agency shall designate a Nodal Officer as the single point of contact.

d. The applicant department/agency shall depute the Nodal Officer and Senior Technical Personnel involved in the software development to consultative meetings, if any, arranged by the SPARK PMU.

e. Once the request for data transfer is approved by SPARK PMU, a Non-Disclosure Agreement (NDA), as prescribed in Annexure B, and a Confidentiality Undertaking, in the format prescribed in Annexure C, shall be duly signed by the authorized person before the data is accessed/transferred.

f. The applicant department shall ensure the security of the services and data shared from SPARK.

g. The applicant department/agency shall conduct security audit of their software application before requesting connectivity with SPARK.

h. After establishing connectivity with SPARK, whenever the applicant department/agency carryout subsequent changes in their software in a manner that would affect the established connectivity, prior written intimation shall be given to SPARK PMU.

i. Continued service requests shall also be routed through SPARK PMU.

V. PROCEDURES TO BE FOLLOWED BY SPARK PMU

a. On receipt of the application from the applicant department/agency, the SPARK PMU shall conduct a preliminary check, and if necessary may forward to the SPARK developer for detailed technical evaluation.

b. The SPARK PMU shall organize technical discussions/seek clarifications from the applicant departments/agencies whenever it is found necessary based on the advice from the SPARK developer.

c. Once the final connectivity plan is mutually agreed among the applicant department/agency, SPARK Developer and SPARK PMU, the SPARK PMU shall issue formal permission to the SPARK Developer to develop and establish connectivity based on the finally approved plan.

d. While on receiving confirmation from the SPARK Developer to formally launch the connectivity, the SPARK PMU shall notify the same to the applicant department/agency.

e. Based on the advice from the SPARK developer, the SPARK PMU shall notify the planned changes in SPARK that may affect the established connectivity in advance to the applicant departments/agencies so that they can also make necessary modifications in their part for the continued connectivity.

f. The responsibility of SPARK PMU shall be limited to the level of technical facilitation alone. The responsibility to ensure the accuracy and authenticity of data shall be with individual departments/agencies and their officers who are authorised to capture data in respect of their employees and process the same in SPARK.

.

VI. PROCEDURES TO BE FOLLOWED BY SPARK DEVELOPER

a. On receiving a request for technical evaluation of a connectivity application from the SPARK PMU, the SPARK developer would examine the application and provide technical advice to SPARK PMU for processing the connectivity application and finalize the connectivity plan with time schedule for completion of the work.

b. After initial evaluation of the application, the SPARK developer shall propose tentative dates for the consultative meetings with the applicant department/agency to finalize the connectivity plan.

c. The SPARK developer shall participate in the consultative meeting arranged by the SPARK PMU and finalize the connectivity plan through discussions. If found necessary, multiple rounds of such meetings shall be conducted.

d. While on receiving the formal approval to the final connectivity plan from the SPARK PMU after the consultative meetings, the SPARK developer would act promptly in accordance with the finalized connectivity plan.

e. The SPARK developer shall test the newly established connectivity in coordination with the development team of the applicant department and confirm to PMU that the connectivity can be formally launched.

f. The SPARK developer shall consider all such established connectivity while plan and implement changes and additions in SPARK. The SPARK developer shall help SPARK PMU to notify such changes in advance to the applicant departments.

g. The SPARK developer shall not directly accept any request for establishing new connectivity with/ data sharing from SPARK. The Developer shall insist all such requests should be routed through Finance (SPARK PMU) Department.

VII. RESTRICTIONS

a. Connectivity shall not be provided to duplicate the functions already available or within the scope of further development of SPARK.

b. Connectivity established with/data shared from SPARK should not be used for any other purpose that is not formally approved by Finance (SPARK PMU) Department.

ANNEXURE A—APPLICATION FORM

APPLICATION FOR ESTABLISHING CONNECTIVITY BETWEEN SPARK AND THE SOFTWARE APPLICATIONS OF OTHER GOVERNMENT DEPARTMENTS/AGENCIES

To

The Chief Project Manager
Project Management Unit (SPARK)
Finance Department
Government of Kerala

<table>
<tr><td>1</td><td>Name of the Department</td><td colspan="4"></td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Name, current designation & PEN/Employee ID of the Head of Department/ Head of the Agency</td><td colspan="2">Name and current designation as in official records</td><td colspan="2">PEN/ Employee ID</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>3</td><td colspan="5">Contact details of the Head of Department/ Head of the Agency</td></tr>
<tr><td></td><td>E-mail</td><td colspan="2"></td><td>Mobile No.</td><td></td></tr>
<tr><td rowspan="2">4</td><td rowspan="2">Name & PEN/ Employee ID of the Nodal Officer designated for the purpose</td><td colspan="2">Name</td><td colspan="2">PEN/ Employee ID:</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>5</td><td colspan="5">Contact details of the Nodal Officer</td></tr>
<tr><td></td><td>Office Address</td><td>Email</td><td>Office Phone</td><td colspan="2">Mobile No.</td></tr>
</table>

6	Name of the software application and/or project for which connectivity with SPARK is requisitioned			
7	A brief description of the scope of the project			
8	Purpose / proposed use of data subsequent to sharing			
9	Government Order Authorising the Data Sharing			
10	Details of the software application and connected database of the requisitioning Department/Agency with which SPARK connectivity is requested			
	Application Development Technology Stack (Frameworks and Platforms)		Database Management System (DBMS) pertaining to the project	
	Date on which the project was launched		Date of latest security audit certification	
11	Required Data Format	API	csv	
12	Frequency of Data Sharing *(One-time / Periodic /*			

	Continuous)	
13	Proposed Data Retention Period	
14	Proposed Mode of Data Transfer [API / Encrypted E-mail / Other Secure File Transfer Modes (Mention the same)]	
15	List out the services/data required from SPARK (in the case of data, all the required data fields with purpose should be listed)	
	Services/Data required	Purpose of such service/data sharing
16	Additional information, if any. If the requisitioning Department/Agency proposes to develop their own API for receiving data/services from SPARK, full technical details of the proposed API should be shared here.	

Declaration

I/We undertake that the data requisitioned pertaining to which the details as specified in the preceding fields are shared,

Shall be used strictly for the stated purpose, and shall not be disclosed, disseminated, transferred, or otherwise transmitted to any third party without prior written approval from Finance (SPARK PMU) Department,

Shall be disposed of/returned upon expiry of the retention period stated above, with the explicit knowledge of Finance (SPARK PMU) Department.

Date: **Office Seal** **Signature of Head of Department**

For Office Use

Approved File Number	
Approved By	
Approved Dated	

ANNEXURE B

Non-Disclosure Agreement (NDA)

This Non-Disclosure Agreement ("Agreement") is made on this .....day of .....(month) , 20..... (Year), between:

SPARK PMU, Finance Department, Govt. of Kerala (hereinafter referred to as the "Data Provider"), represented by Sri / Smt ....., its Chief Project Manager (As per Circular No.70/2026/Fin dated 18.11.2026), (which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors) of the FIRST PART;

AND

[Name of Vendor/Agency/Entity], having its office at [Address] represented by <mention name and designation>*, (hereinafter referred to as the "Data Recipient"), (which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors) of the SECOND PART.*

(The Data Provider and Data Recipient are hereinafter collectively referred to as the "Parties" and individually as “Party”.)

NOW, THEREFORE , in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:-

1. **Purpose**

   This Agreement governs the sharing of digital data by the Data Provider with the Data Recipient for the purpose of *[state specific purpose as in column 8 of Annexure A]* , and sets out the obligations of the Data Recipient with respect to confidentiality, security, and permitted use of such data in line with provisions of The Digital Personal Data Protection (DPDP) Act, 2023.

2. **Permitted Use**

a. The Data Recipient shall use the data solely for the purpose stated in Clause 1 and for no other purpose whatsoever.
b. The Data Recipient shall not sell, license, lease, rent, publish, disclose, transfer, assign, or otherwise commercially exploit, distribute, or make available the Data, in whole or in part, to any third party without the prior written consent of the Data Provider.

c. The Data Recipient shall not share, transfer, or grant access to the data to any sub-contractor or third party without the prior written consent of the Data Provider.

3 . **Protection of Confidential Information-** With respect to any Confidential Information disclosed to it or to which it has access, Data Recipient affirms that it shall:

i. Use the Confidential Information as necessary only in connection with purpose stated in Clause 1 in accordance with the terms and conditions contained herein;
ii. Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Information than the parties take to protect the confidentiality of its own proprietary and confidential information. The Data Recipient shall ensure that any employees or representatives with access to such information are bound by confidentiality obligations not less restrictive than those herein, and shall remain fully liable for any breach by such employees or representatives.

iii. Not to make or retain copies of any details of results of any information, tests, analysis, extracts or usages carried out by the Data Recipient in connection with the Data Provider's products and/or services, IT infrastructure, etc. without the express written consent of Data Provider.

iv. Not to disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the

express written consent of the Data Provider;

v. Return to the Data Provider, or destroy, at Data Provider's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof immediately on (i) expiration or termination of this agreement, or (ii) the request of Data Provider therefor.

vi. The Data Recipient covenants and agrees that, it shall not, under any circumstances, transfer, transmit, store, process, analyze, or otherwise handle any Confidential Information, data, or personal data of the Data Provider or any part thereof, outside the territorial boundaries o f India, whether directly or indirectly, without obtaining the prior, explicit, and written consent of the Data Provider.

vii. The Data Recipient shall implement appropriate access-control mechanisms, including Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC), with the principle of least privilege enforced. All transmission of Data over networks shall be secured using TLS 1.2 or higher, with TLS 1.3 preferred. Data shall not be transmitted through ordinary email, unsecured file-sharing mechanisms, or any other unencrypted channel. Data shall be shared only through mutually approved secure file-transfer mechanism, as specified in Column 14 of Annexure A. The Data Recipient shall promptly notify the Data Provider of any actual or reasonably suspected unauthorised access, disclosure, loss, compromise or security breach involving the Data and shall take measures to contain, mitigate and remediate such incident.

viii. Not to engage or appoint any non-resident/foreigner to undertake any activity related to information Security.

ix. The Data Recipient shall not disclose, discuss, or disseminate to any member of the public, media, press, or any third party, any information regarding the existence, nature, or terms of the arrangement entered into between the Data Recipient and the Data Provider.

x. Make sure that all the employees and/or consultants engaged to undertake any activates on its behalf have signed the mandatory non-disclosure agreement.

xi. No sub-sharing or further transfer of data to any other department,

agency, public without prior written departmental approval.

4. **Security Obligations of the Data Recipient**

i. All Data stored by the Data Recipient shall be protected using AES-256 encryption and all transmission of Data over networks shall be secured using TLS 1.2 or higher, with TLS 1.3 preferred.
ii. Restrict access to the data strictly to personnel who require it for the stated purpose, on a need-to-know basis.
iii. Maintain access logs and make them available to the Data Provider upon request.
iv. Implement reasonable administrative, technical, and physical safeguards to prevent unauthorized access, loss, or disclosure.

5. **Data Breach Notification**

The Data Recipient shall notify the Data Provider of any actual or suspected unauthorized access, disclosure, loss, or breach involving the shared data within [24-72] hours of becoming aware of such an incident, and shall cooperate fully with any subsequent investigation.

6. **Data Retention and Return/Destruction**

The Data Recipient shall retain the data only for the period specified in **Annexure A** or the duration of the underlying contract, whichever is shorter. Upon expiry of this period, termination of the underlying contract, or written demand by the Data Provider, the Data Recipient shall, at the Data Provider's option, return all data and copies thereof or certify in writing the complete and irrecoverable destruction of the same, within [15] days.

7. **Ownership and Intellectual Property**

All data shared under this Agreement, and any copies thereof, shall remain the sole and exclusive property of the Data Provider at all times. Nothing in this Agreement shall be construed as granting or transferring any ownership rights, intellectual property rights, or licenses to the Data Recipient.

8. **Liability and Indemnity**

The Data Recipient shall indemnify and hold harmless the Data Provider against any loss, damage, liability, penalty, litigation costs or claim arising from the Data Recipient's breach of this Agreement, including but not limited to, any unauthorized access, use, disclosure, modification, or loss and destruction of the Data.

9. **Audit Rights**

The Data Provider, or an auditor nominated by it, shall have the right to audit the Data Recipient's compliance with this Agreement upon reasonable prior notice.

10. **Amendments**

No amendment, modification, variation, waiver and/or discharge of this Agreement shall be valid, effective or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.

11. **Binding Agreement**

This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

12. **Severability**

It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall

not affect the other provisions of this Agreement.

13. **Waiver**

Waiver by either party of a breach of any provision of this Agreement, shall not be deemed to be a waiver of any preceding or succeeding breach of the same or any other provision hereof.

14. **Survival**

Both parties agree that all of their obligations undertaken herein with respect to Confidential lnformation received pursuant to this Agreement shall survive in perpetuity even after expiration or termination of this Agreement.

15. **Term and Termination**

This Agreement shall remain in force for the duration of *[the underlying contract / a specified term]*, and may be terminated by the Data Provider with immediate effect in the event of a material breach, including any unauthorized disclosure or misuse of the data.

16. **Governing Law and Jurisdiction**

This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India, including the The Digital Personal Data Protection (DPDP) Act, 2023, and the parties hereby unconditionally agree that, the courts and/or forums situated at Thiruvananthapuram, Kerala, shall have exclusive jurisdiction to settle any disputes arising out of or in connection with this Agreement.

17. **Term**

This Agreement shall come into force on the date of its signing by both the parties.

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

18. **Signatures**

Name: Designation Date:	Name: Designation Date:
(Data Provider)	**(Data Recipient)**

WITNESSES:

1.

2.

WITNESSES:

1.

2.

Annexure C: Confidentiality Undertaking Format

(To be signed by Head of Department / Nodal Officer)

I, the undersigned, **Head of Department / Nodal Officer**, being the authorized officer representing the Department/Agency and having been granted access to certain confidential data for the purpose of the assignment described above, hereby undertake and declare that:

1. The 'Data' shall be accessed and used solely for the purpose for which access has been authorized and strictly in connection with the aforesaid assignment.
2. The Department shall ensure that the 'Data' is not copied, reproduced, transmitted, shared, or disclosed, in whole or in part, to any person or entity who is not duly authorized to receive or access such data.
3. The 'Data' shall not be stored on any personal device, personal email account, external storage/portable media, unsanctioned cloud storage repositories, or other unauthorized information-sharing platforms.
4. Any actual or suspected unauthorized access, loss, alteration, misuse, or disclosure of the 'Data' coming to the knowledge of the Department shall be reported immediately to the Data Fiduciary.
5. The Department shall ensure that all officers, employees, consultants, or other authorized personnel having access to the 'Data' comply with the applicable confidentiality, data protection, information security, and access control requirements.
6. I understand and acknowledge that any breach of this undertaking shall attract appropriate disciplinary, administrative and legal action and shall also result in imminent termination of the relevant contract/engagement, and such conduct shall entail civil and/or criminal consequences in accordance with the applicable law.
7. This undertaking shall remain binding even after completion, termination, or expiry of the assignment/engagement/contract, in so far as the confidentiality and protection of the data accessed are concerned.

I hereby certify that the above undertaking is given on behalf of the Department and that the data accessed shall be handled strictly in accordance with the applicable Government instructions, confidentiality requirements, and information security policies.

Name: _____

Designation: _____

Name of Department/Office: _____

Signature: _____

Date: _____

Official Seal: _____