LIC PFL
LIC PENSION FUND LTD

Response to Pre-Bid Queries for the RFP Document for Procurement of Enterprise Cloud-Based Data Loss Prevention (DLP) Solution for Endpoint DLP & Email DLP dated 11.08.2026.

SN	RFP Document Reference(s) (Section &Page Number)	Clause (in brief) of RFP requiring clarification(s)	Brief details/ Query in reference to the clause	Response
1	Section 7.2(a) – Endpoint DLP – Capabilities	Monitor file copy, move, rename, delete and encryption activities.	Request to remove/modify this requirement from the DLP scope. It may be revised as "The solution should monitor and control sensitive data movement and policy violations across endpoints, removable media, network shares, and other communication channels." Justification: Monitoring all file-system operations such as move, rename, and delete is an endpoint auditing/forensic capability rather than a standard DLP function.	No Change
2	Section 7.2(a) – Endpoint DLP – Capabilities	Monitor local folders, shared folders and mapped network drives.	Request to amend this point as: Monitor Network share and local drives. Justification: Monitoring generic shared folders and mapped network drives is primarily an endpoint/file-system monitoring capability and is not a core DLP functionality.	No Change
3	Section 7.2(b) – Email DLP – Capabilities	Monitor inbound and outbound email communications.	Kindly amend this point as: Monitor outbound email communications. Justification: DLP solutions are primarily designed to monitor and control outbound data flows to prevent unauthorized disclosure or exfiltration of sensitive information. Inbound email monitoring is generally addressed by email security/secure email gateway solutions rather than DLP.	No Change
4	Section 7.2(b) – Email DLP – Capabilities	Block, quarantine, encrypt or monitor unauthorized email transmission.	Kindly amend this point as: Block, quarantine or monitor unauthorized email transmission. Justification: Email encryption requires a dedicated encryption module/license. Hence, we request to remove the 'encrypt' functionality from this requirement.	No Change

5	Section 7.2(b) – Email DLP – Capabilities	Integrate with Microsoft 365, Exchange, Active Directory/LDAP and SIEM/SOC.	Justification: Microsoft 365 monitoring may require an Outlook add-in or Microsoft 365-native DLP capability, which may involve additional licensing/modules. Hence, we request that Microsoft 365 integration be removed from the mandatory DLP requirement or considered as an optional capability.	No Change
6	Section 7.2(c) – Web DLP (Browser / Upload Monitoring) – Capabilities	Monitor and control file downloads based on organizational policies.	Kindly amend this point as: Monitor and control file Uploads based on organizational policies. Justification: File download monitoring is generally not a core DLP functionality, as DLP solutions primarily focus on preventing the unauthorized upload, transfer, or exfiltration of sensitive data.	The Section mentioned in the query doesn't exist in RFP, hence we are unable to comment.
7	Section 7.3(a) – Common Functional Requirements – Data Discovery & Classification	Automatic and manual discovery of sensitive information across endpoints, file servers, network shares, databases, cloud repositories and collaboration platforms.	Kindly amend this point as: automatic and manual discovery of sensitive information across endpoints and supported data repositories. Justification: Discovery across databases, cloud repositories and collaboration platforms may require separate connectors, integrations or additional modules depending on the platform and deployment architecture.	No Change
8	Section 7.3(a) – Common Functional Requirements – Data Discovery & Classification	Support classification labels such as Public, Internal, Confidential, Restricted, Secret or organization-defined labels.	Kindly amend this point as: Support data classification based on organization-defined policies and classification criteria. Justification: Classification labels such as Public, Internal, Confidential, Restricted and Secret are organization-specific and may vary across implementations. A DLP solution should support policy-based data classification rather than mandate predefined classification labels.	No Change
9	Section 7.3(b) – Common Functional Requirements – Policy Management & Enforcement	Support user, group, department, device, application, content, context, location, time and risk-based policies.	Kindly amend this point as: Support user, group, department, device, application, content, context, location. (Request to remove time & risk-based policies.)	No Change

10	Section 7.3(c) – Common Functional Requirements – Data Protection Coverage (Data in Use)	File Copy	Kindly remove this point from the DLP scope. Justification: Generic file copy monitoring is primarily an endpoint file-system activity monitoring capability and is not a core DLP requirement. DLP solutions are primarily designed to monitor and control the unauthorized movement or exfiltration of sensitive data based on defined policies.	No Change
11	Section 7.3(c) – Common Functional Requirements – Data Protection Coverage (Data in Use)	File Move	Kindly remove this point from the DLP scope. Justification: Generic file Move monitoring is primarily an endpoint file-system activity monitoring capability and is not a core DLP requirement. DLP solutions are primarily designed to monitor and control the unauthorized movement or exfiltration of sensitive data based on defined policies.	No Change
12	Section 7.3(c) – Common Functional Requirements – Data Protection Coverage (Data in Motion)	Cloud Applications	Kindly remove this point from the DLP scope. Justification: Monitoring and controlling cloud applications is primarily a CASB (Cloud Access Security Broker) functionality and is not part of the core DLP solution.	No Change
13	Section 7.3(c) – Common Functional Requirements – Data Protection Coverage (Data in Motion)	Collaboration Platforms	Kindly remove this point from the DLP scope. Justification: Monitoring and controlling collaboration platforms is primarily a CASB (Cloud Access Security Broker) functionality and is not part of the core DLP solution.	No Change
14	Section 7.3(d) – Common Functional Requirements – Data Exfiltration Prevention	Collaboration Platforms	Kindly remove this point from the DLP scope. Justification: Monitoring and controlling collaboration platforms is primarily a CASB (Cloud Access Security Broker) functionality and is not part of the core DLP solution.	No Change