Attachment A

Baseline Functional Requirements

A Baseline Template for Secure Enterprise Browser Platform (SEBP)

Attachment A

Baseline Functional Requirements - Secure Enterprise Browser Platform (SEBP)

1. Purpose

This document defines the **baseline functional requirements** for a **Secure Enterprise Browser Platform (SEBP)** to be procured and delivered as a **Software-as-a-Service (SaaS)** solution.

These requirements are intended to:

- Provide a common baseline for vendor responses
- Ensure coverage of core SEBP capabilities across security, usability, and manageability
- Support consistent evaluation and comparison of proposed solutions

Agencies may add additional requirements, use cases, or configurations where appropriate, provided they remain consistent with the SaaS model described in the RFQ.

2. Scope

The SEBP will:

- Secure and monitor web and SaaS application access for users across **managed and unmanaged devices**
- Enforce data protection and usage policies within the browser/session
- Provide visibility into user activity and security-relevant events
- Integrate with the agency's existing identity, security, and logging ecosystem
- Be delivered and operated **solely as a cloud-hosted SaaS solution** (no on-premise or hybrid deployment)

3. Baseline Functional Requirements

3.1 General SaaS & Platform Requirements

The Solution **must**:

1. Operate as a **cloud-hosted SaaS platform**, fully managed and maintained by the Contractor.
2. Provide a centralized **administrative console** for configuration, policy management, and monitoring.
3. Support **role-based access control (RBAC)** for administrative functions (e.g., global admin, security admin, helpdesk, read-only reporting).
4. Provide a **multi-tenant or logically isolated** architecture that securely separates each Customer's data from other customers.
5. Deliver **continuous updates and improvements** without requiring Customer-hosted infrastructure or manual upgrades.
6. Support **scaling to the agency's projected user population** and growth across additional agencies covered by the Contract Award.
7. Provide **high availability** and resilience consistent with the uptime targets defined in the RFQ's Service Level section.

8. Provide **documentation** for platform capabilities, configuration options, and administrative tasks.

3.2 Browser Security & Data Protection

The Solution **must** provide fine-grained **data protection and usage controls** at the browser/session level, including:

1. Ability to **inspect and enforce policy** on web and SaaS application access based on:
    - User identity and group/role
    - Device posture or classification (where supported)
    - Network location or IP range
    - Target application, URL, or resource
2. Ability to **control data movement** within the browser, including:
    - Restricting or allowing **copy/paste** operations
    - Restricting or allowing **file downloads** from specific applications or categories
    - Restricting or allowing **file uploads** to specific applications or categories
    - Controlling or disabling **printing** from browser sessions
    - Restricting or monitoring **screenshot** and screen-capture behavior (where technically feasible)
3. Ability to define and enforce **context-aware policies**, such as:
    - Stricter controls for unmanaged devices
    - Different controls for internal vs. external applications
    - Additional protections for applications handling regulated or sensitive data
4. Ability to enforce **web isolation / session isolation** as appropriate for high-risk sites or applications.
5. Ability to apply **data protection controls consistently** across supported browser environments (e.g., Chrome, Edge, and other supported modern browsers), subject to vendor capabilities.

3.3 Identity, Access & Session Control

The Solution **must**:

1. Integrate with the agency's **Identity Provider (IdP)** for **Single Sign-On (SSO)** using standards such as SAML 2.0 and/or OpenID Connect.
2. Support **Multi-Factor Authentication (MFA)** as enforced by the existing identity platform or agency MFA solution.
3. Support **user and group-based policy enforcement** leveraging directory attributes (e.g., role, department, group membership).
4. Provide **session-level controls**, including the ability to:

    - Terminate active sessions based on policy
    - Require re-authentication based on risk/context
    - Apply different enforcement policies for high-risk applications or behaviors

5. Support **managed and unmanaged devices**, with the ability to apply differentiated policy per device context where supported (e.g., via device certificates, MDM enrollment, or other posture mechanisms).

3.4 Compliance & Security Standards (Jurisdiction-Selectable)

The Solution **must** support alignment with relevant security and compliance requirements. The agency will specify which apply in the RFQ or Contract Award.

At a minimum, the Solution must:

1. Follow **industry-standard security practices** for cloud services, including:
    - Encryption **in transit** (e.g., TLS 1.2 or higher)
    - Encryption **at rest** for stored data
    - Secure development practices and vulnerability management

2. Provide **audit logs** sufficient to support security investigations and compliance obligations.

Where applicable (to be selected by the agency), the Solution should:

- Align with or support frameworks such as **NIST CSF**, **NIST SP 800-53**, **StateRAMP/FedRAMP**, **CJIS**, **HIPAA**, **FERPA**, or other jurisdiction-specific frameworks.
- Provide documentation indicating current certification status, attestation (e.g., SOC 2, ISO 27001), or equivalent evidence of security controls.

  Note: Agencies should only select the minimum necessary frameworks in the RFQ or Contract to avoid imposing unnecessary cost or excluding capable vendors.

3.5 Integration & Compatibility

The Solution **must** support integration with key components of the agency's security and operations stack, including:

1. **Identity and Access Management:**
    - Integration with one or more IdPs (e.g., Azure AD, Okta, etc.) for SSO and user/group synchronization.
    - Support for SCIM or equivalent for user provisioning/deprovisioning, where available.

2. **Logging & SIEM:**
    - Ability to export logs and events (e.g., access, policy enforcement, security-relevant events) to common SIEM platforms in standard formats (e.g., syslog, JSON, or vendor-supported APIs).

3. **Ticketing / IT Service Management (ITSM):**
    - Optional integration to create or update incidents/tickets based on SEBP events (e.g., ServiceNow, Jira Service Management, or equivalent).

4. **Secure Web Gateway / Network Security (If Applicable):**
    - Optional integration or coexistence with existing secure web gateway or firewall tooling where appropriate.

3.6 Performance & Availability

The Solution must:

1. Support a level of **monthly uptime** consistent with the RFQ's selected SLA option (e.g., 99.999% or 99.999% monthly uptime).
2. Include a documented approach for **service degradation** handling (partial outages, performance issues) and **service restoration**.
3. Provide performance that allows reasonable end-user experience for web and SaaS applications under typical agency network conditions.

Higher availability targets (e.g., **99.999%**) may be required by the agency for high-criticality environments and will be specified in the RFQ's Service Level section.

3.7 Monitoring, Logging & Reporting

The Solution **must** provide robust monitoring and reporting capabilities, including:

1. **Event Logging:**
    - User session activity logs (logins, logouts, session duration).
    - Policy enforcement events (blocked/allowed actions, policy violations).
    - Security-relevant events (e.g., attempts to copy sensitive data, blocked uploads/downloads, suspicious browser activity).

2. **Administrative Activity Logging:**
    - Changes to policies and configurations.
    - Administrator logins.
    - Role or permissions changes.

3. **Reporting:**
    - Pre-built dashboards for security, adoption, and usage.
    - Ability to filter and search logs by user, device context (where available), application, and time range.
    - Ability to export reports or raw logs for further analysis.

4. **Retention:**
    - Configurable log retention period, either within the platform or via integration with external logging/SIEM services, consistent with agency policy.

3.8 Training & Support

The Solution must include:

1. **Administrator Training:**
    - Training for system administrators and security staff on configuration, policy design, troubleshooting, and reporting.

2. **End-User Awareness Materials:**
    - Documentation or short guides explaining any end-user impact (if user experience meaningfully differs from standard browser usage).

3. **Support Services:**
    - Access to vendor support during business hours at a minimum, with options for extended coverage if needed.
    - Clear escalation paths and documented response and resolution targets aligned with the RFQ's SLA section.

Training may be delivered through a combination of live sessions, recordings, and self-service documentation.

3.9 Optional & Value-Added Services

The following capabilities are **optional**, but may be requested or scored by agencies:

1. **Policy Advisory Services:**
    - Assistance in designing and tuning SEBP policies tailored to agency risk and use cases.

2. **Managed Administration:**
    - Vendor-provided or partner-provided ongoing administration and policy management under defined SOWs.

3. **Advanced Analytics & Risk Scoring:**
    - Enhanced insights into risky users, applications, or behaviors beyond standard dashboards.

4. **Sandbox / Test Environment:**
    - Optional non-production environment for testing new policies and configurations.

5. **Quarterly Business Reviews (QBRs):**
    - Regular meetings to review performance, adoption, and recommendations.

Agencies may specify which of these optional services they wish to include in their RFQ or evaluation criteria.

4. Vendor Response Matrix (Recommended Format)

Vendors should indicate how their Solution meets each baseline requirement, and may provide additional detail where necessary. Agencies can adapt this matrix as needed.

Ref ID	Requirement Summary	Mandatory (Y/N)	Vendor Response (Meets / Partially Meets / Does Not Meet)	Notes / Explanation / Reference
BR-1.1	SaaS-only, cloud-hosted delivery	Y/N		
BR-1.2	Central administrative console	Y		
BR-2.1	Copy/paste, download, upload, print, screenshot controls	Y		
BR-2.2	Context-aware policy (identity, device, network, app)	Y		
BR-3.1	SSO with agency IdP	Y		
BR-3.2	MFA support (via existing IdP/MFA)	Y		
BR-4.x	Compliance alignment (as selected by agency)	As defined		
BR-5.1	Integration with SIEM/logging tools	Y		
BR-5.2	Integration with ITSM (optional)	N		
BR-6.1	Uptime target consistent with RFQ SLA	Y		

BR-7.1	Logging of user and policy events	Y		
BR-7.2	Dashboards and reporting	Y		
BR-8.1	Admin training	Y		
BR-9.1	Optional services (if requested in RFQ)	N		