ID	Category	Sub Category	Requirement Statement (Specific and Measurable)	Evidence / Verification Method	MoSCoW
1	Availability & Disaster Recovery		The solution must be available for business use every day during hours 7:00 - 20:00 under normal operating conditions, with a minimum monthly system availability of 99,5%. Availability must be measured using an agreed monitoring method and must exclude agreed maintenance windows. Recovery objectives (RTO/RPO) must be aligned with the supplier's business continuity and disaster recovery objectives for the service.	Uptime/availability reports for at least The last 12 months; definition of measurement method (in-/exclusion of maintenance); BCP/DRP documentation showing RTO/RPO forThe Enexis service.	Must
2	Availability & Disaster Recovery		The solution must achieve an annual service availability of at least 99,5% under normal operating conditions, measured over a rolling 1 month period using agreed availability metrics, excluding agreed maintenance windows. These targets must be formally included in the SLA.	Annual availability summary (rolling 12 months) with calculation method; signed SLA including availability KPI and definitions; examples of monthly SLA reports provided to customers.	Must
3	Availability & Disaster Recovery		Downtime in the production environment for updates or changes may only occur after prior written agreement with Enexis. The supplier must give at least 10 working days' notice, including an impact analysis, planned timing and expected duration, and follow a documented change management process.	Change management procedure; examples of change records for production deployments showing notification to Enexis ≥5 working days in advance; release/maintenance calendar.	Must
4	Availability & Disaster Recovery	Incident Management	For incidents with the highest priority (as defined in the SLA), the supplier must achieve a Mean Time To Respond (MTTResp) of at most 15 minutes, measured from registration of the incident in the service desk system until the first substantive response by qualified support staff. This must apply on workdays during working hours 7:00 - 20:00 for all in-scope services.	Incident management policy; SLA with defined priority levels and MTTResp; incident ticket samples with timestamps (registration vs. first response) showing compliance withThe 15-minute target.	Must
5	Availability & Disaster Recovery	Incident Management	For highest-priority incidents that cause unavailability of the service, the supplier must achieve a Mean Time To Repair (MTTR) of at most 4 hours, measured from incident registration to full restoration of the agreed service functionality, in line with the supplier's incident and continuity procedures.	SLA with MTTR-agreements for P1/P0 incidents; incident reports showing actual repair times; overview of major incidents with timelines for last 12 months.	Must
6	Availability & Disaster Recovery	Backup & Recovery	The supplier must implement backup and/or replication mechanisms so that the Recovery Point Objective (RPO) for production data is at most ≤5 minutes. This is measured as the maximum time between the last consistent restore point and the moment of a disruption.	Technical architecture and backup/replication design; configuration of backup/replication frequency; DR/restore test reports showing actual RPO achieved ≤ 5 minutes for Enexis data.	Must
7	Availability & Disaster Recovery	Backup & Recovery	For critical services, the supplier must ensure a Recovery Time Objective (RTO) of at most 8 hours, measured from the start of a disruption (service unavailable) until the service is fully available again for end users. This must be verified by at least 1 annual disaster recovery test.	BCP/DRP including defined RTO per service; DR test schedule; DR test reports showing actual recovery time ≤ 8 hours forThe Enexis service.	Must
8	Availability & Disaster Recovery	Backup & Recovery	The supplier must maintain and periodically test a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) that cover service continuity during physical disasters (e.g. flooding, fire), including loss of the primary site and/or critical staff. These scenarios must be reviewed and tested at least annually.	BCP/DRP documents including calamity scenarios; annual BCP/DRP review records; test reports for at least one scenario involving loss of site or infrastructure.	Must
9	Availability & Disaster Recovery	Availability & Disaster Recovery	Where technically feasible, planned maintenance must be performed without functional downtime for end users by using high-availability or failover mechanisms. If downtime cannot be avoided, maintenance must follow the agreed change process and be pre-approved and scheduled with the customer.	Change and release management procedure; architecture showing HA/failover setup; examples of maintenance windows with evidence (monitoring) that no user downtime occurred; where downtime: approval evidence.	Should
10	Backup & Recovery	Backup & Recovery	The solution must support data archiving in line with the agreed retention periods and data classifications. Archived data must remain retrievable and protected at an appropriate security level, and data must be deleted or anonymised once the retention period has expired.	Archiving functionality documentation; configuration of retention and archiving rules; sample evidence of archived data retrieval and of deletion/anonymisation after retention period; data retention policy.	Must
11	Backup & Recovery	Backup & Recovery	The solution must provide backup and recovery capabilities for all customer data with a minimum retention period of 30 days. It must be possible to restore data to any point within this 30 day window, including both archived and transactional data, in line with agreed retention schedules.	Backup and retention policy; backup configuration showing ≥30 days retention; restore test reports demonstrating successful recovery of data older than 30 days; documentation of handling of backups in exit/deletion scenarios.	Must
12	Client & Device		The solution must work for end users without functional limitations on laptops, tablets and smartphones that meet the customer's workplace standards. The supplier must provide user guidance and training material describing any device specific limitations or configuration requirements needed for secure and effective use.	User and admin documentation describing supported device types and configurations; test reports or matrices showing device/OS/browser combinations; training and awareness material for end users and admins.	Must
13	Client & Device		The user solution must be independent of the physical workplace and must not require any local installation of software components on user devices, other than standard centrally managed components approved by the customer. Access must be possible only via centrally controlled mechanisms (e.g. browser, managed app stores, virtual desktop).	Technical architecture description (web/SaaS/VDI); client requirements list; confirmation that no unmanaged local agents or plugins are required; deployment documentation or packaging guidelines used for Enexis.	Must
14	Client & Device		The user solution must be fully functional and supported on the current standard workplace based on supported operating systems (and successor versions within the N-1 support strategy). Required client-side patches and security updates must be applied in a timely manner to maintain secure and stable operation.	Workplace standard documentation; supplier support statement listing of actual and supported versions of operating systems; test reports (FAT/UAT) on Enexis devices; patch compliance reports for client components (if any).	Must
15	Client & Device		The user solution must be fully functional and supported on Android devices from actual supported Android versions, in line with the customer's mobile standards. The supplier must clearly document any limitations and security requirements (such as MDM, minimum OS level, required security settings) for managed Android devices.	Supplier's official support matrix for mobile OS versions; mobile device management (MDM) policy settings required forThe app; test reports on Enexis devices used in Enexis context.	Must
16	Client & Device		The user solution must be fully functional and supported on iOS devices from actual and supported iOS versions, in line with the customer's mobile standards. The supplier must clearly document any limitations and security requirements (such as MDM enrolment, minimum OS version, device protection settings) for managed iOS devices.	Supplier's official support matrix for iOS versions; MDM policy/configuration forThe app; test reports on Enexis devices in representative Enexis configurations.	Must
17	Client & Device		If the solution is web-based, it must be fully functional and supported on current, vendor-supported versions of Microsoft Edge and Google Chrome used by the customer. End-of-life browsers may only be used if risks are clearly documented and explicitly accepted by the customer.	Browser support statement from supplier; test reports onThe current Enexis standard browsers; documented risk assessment for any legacy browser support (if applicable); secure coding guidelines aligning with browser support.	Must
18	Client & Device		The solution should be browser-independent. It must be designed and tested to operate correctly on the main browsers defined in the customer's workplace standard (e.g. Edge, Chrome and, where applicable, Safari), with a documented list of supported browsers and any known limitations or exceptions.	Browser compatibility matrix; results of regression tests across supported browsers; documentation of known browser-specific issues and workarounds; secure web development guidelines referencing cross-browser testing.	Should
19	Client & Device		The solution must support distribution via centrally managed mechanisms (for example software distribution tools, controlled mobile app stores, or virtual desktop images), enabling automated deployment and updates to user workplaces and devices in line with the customer's change and release processes.	Deployment and packaging documentation (MSI, AppX, mobile app store metadata, etc.); examples of automated rollout scripts or configurations; change management records for releases to Enexis environments.	Must
20	Client & Device		The user interface of the solution must be responsive and adapt to different screen sizes and orientations without loss of readability or functionality. It must support touch interaction on devices used by the customer, and the UX must be designed and tested according to agreed UX principles and documented user interface standards.	UX design documentation; responsive design specifications; test reports (including screenshots) for different resolutions and touch devices; reference to Enexis UX principles and howThey are implemented inThe solution.	Must
21	Support		The supplier must provide appropriate information security and privacy awareness and training to all staff and relevant contractors involved in delivering the service. Training must be provided at onboarding and at least annually, and should include how to use any accessibility features of the solution (such as high-contrast modes or enlarged fonts) in a secure and correct way.	Training and awareness plan; training materials (slides/e-learning) including references to secure and correct use ofThe solution; attendance/completion statistics for staff working onThe Enexis service.	Must
22	Client & Device		The supplier must design and maintain the user experience (UX) of the solution according to agreed UX principles. The supplier must document how the solution meets or deviates from these principles, obtain customer approval for deviations, and ensure that UX changes follow the secure development and change management process.	UX guidelines mapping document (Enexis UX principles vs. actual implementation); design reviews; approval records from Enexis for deviations; change records for UX changes showing review and approval.	Should
23	Integratie	Application & API Security	The solution must support secure integration with customer systems via web services, offering authenticated and authorised interfaces (as a provider) and the ability to consume web services (as a consumer). Network segmentation and access control must be used so that only authorised systems can connect.	API/interface documentation; architecture diagrams showing provider/consumer integrations; configuration of authentication/authorisation for web services; network diagrams with segmentation and firewall rules for integration flows.	Must
24	Integratie	Application & API Security	All web services and APIs used for the service must be provided as secure RESTful APIs or SOAP web services, and must be designed and configured with secure coding and network practices, including authentication, authorisation, input validation and logging.	API specifications (OpenAPI/Swagger, WSDL); secure coding guidelines; sample configuration for authentication/authorisation; security test reports (SAST/DAST) covering API endpoints; network and firewall configuration documents.	Must
25	Integratie	Application & API Security	All APIs and web services offered or used by the solution must be fully documented, including endpoint descriptions, data models, authentication and authorisation mechanisms, error handling, and versioning. API documentation must be kept up to date as part of the software development lifecycle.	API documentation (developer portal, manuals, OpenAPI/Swagger); change history for API versions; SSDLC documentation showing how API documentation is maintained; sample release notes including API changes.	Must
26	Integratie	Application & API Security	For all RESTful APIs provided as part of the solution, the supplier must provide machine-readable API specifications using Swagger 2.0 or OpenAPI 3.1.0 These specifications must be kept in sync with the implemented APIs and made available for integration, testing and security review.	Swagger/OpenAPI files (JSON/YAML); location/URL of API documentation; process description for keeping Swagger/OpenAPI specs in sync with implementation; sample comparison between implementation and specification.	Should
27	Monitoring & Logging	Logging & Monitoring	The solution must present error messages that are understandable for administrators and support staff, containing sufficient technical detail (for example error codes, correlation IDs) for troubleshooting, while not exposing sensitive information to end users. Error messages must be defined and tested as part of the development process.	Error handling design documentation; examples of user-facing and admin-facing error messages; logging format including correlation IDs; test cases demonstrating correct masking of sensitive data in error messages.	Must
28	Monitoring & Logging	Logging & Monitoring	The solution must log all system errors that affect the customer, including at least a timestamp, severity, component, correlation ID and, where possible, affected users. Logs must be protected against unauthorised access and modification, centrally retrievable, and use a reliable time source so that events can be correlated across systems.	Logging policy; application and infrastructure log configuration; sample log files showing required fields; configuration of NTP/time synchronisation; evidence of central log collection or SIEM integration for Enexis.	Must
29	Monitoring & Logging	Logging & Monitoring	The solution must support integration with customer monitoring tools by exposing relevant system health and performance metrics (for example CPU, memory, disk, service availability) through documented interfaces or agents.	Monitoring integration design; list of available metrics and endpoints/agents; documentation for connecting to Enexis monitoring platform; sample monitoring dashboards or alerts usingThese metrics.	Must
30	Monitoring & Logging	Logging & Monitoring	The solution must provide metrics and logs on database health (such as connections, locks, long-running queries and resource usage) and relevant security events, accessible in a secure manner to the customer or their monitoring tools.	Database monitoring configuration (DMVs, performance counters, audit logs); documentation of available monitoring endpoints or integrations; sample monitoring reports or alerts for database performance and security events.	Must
31	Monitoring & Logging	Logging & Monitoring	The solution must support monitoring of key business processes (for example workflow status, queue lengths, failed steps) by exposing process metrics and events that can be monitored and alerted upon, so that process interruptions can be detected and resolved within agreed continuity targets.	Process architecture and description of key business processes; list of process metrics/events exposed byThe solution; examples of monitoring dashboards or alerts for process failures; change records showing onboarding of new processes into monitoring.	Must
32	Monitoring & Logging	Logging & Monitoring	The solution must clearly distinguish between functional and technical failures in error handling and logging (for example using separate error codes or categories), so that functional issues are routed to business support and technical issues to IT support. This classification must be defined, implemented and tested as part of the development lifecycle.	Error classification scheme (functional vs technical); logging format showing category/type; examples of tickets or incidents with correct categorisation; SSDLC documentation including error handling design and test cases.	Must
33	Monitoring & Logging	Logging & Monitoring	The solution must provide clear insight into technical failures by capturing adequate technical details in logs (for example stack traces, component identifiers, timestamps, correlation IDs) that are accessible to the supplier's support teams. The solution must support efficient handling of these failures through integration with incident and problem management tools.	Logging and monitoring policy; sample technical error logs with required fields; documented integration with incident/problem management tools; examples of incident records linking to technical log entries and root cause analyses.	Must
34	Performance		Under normal operating conditions (agreed workload, data volume and network conditions), refresh actions within the application (for example reloading data or dashboards) must have a response time ≤2 seconds for at least 95% of measurements, measured from the user or system trigger until the content is fully updated and usable.	Performance test plan defining "refresh" actions and workload; performance test results showing 95th percentile refresh time ≤ 2 seconds; monitoring data or APM dashboards demonstrating compliance in production for key refresh actions.	Must
35	Performance		The solution must support dynamic scaling of storage and processing capacity (scale-out and/or scale-up) based on observed or forecast load, so that agreed performance targets are met at defined peak usage levels.	Capacity management plan; architecture showing scalability mechanisms; results of load/stress tests at agreed peak concurrency; configuration of auto-scaling or scaling procedures; monitoring showing resource utilisation vs capacity.	Must
36	Platform	Network & Infrastructure Security	The solution must be accessible via the internet so that users can access it from non-corporate locations. At the same time, all processing and storage of personal data must remain within locations agreed with the customer and must use secure network connections and access controls.	Network and security architecture (including DMZ, VPN, secure remote access); list of processing locations maintained in Appendix 3 – Locaties Informatie; evidence of secure protocols (e.g. TLS), access controls and geolocation restrictions.	Must
37	Platform	Supplier / Cloud Security	The solution must be delivered as a cloud-based service (preferably SaaS, otherwise PaaS/IaaS). All third-party cloud providers and sub-suppliers involved in delivering the service must be contractually required to meet the agreed security and privacy requirements, and must be recorded in an up-to-date register including their locations, roles and responsibilities.	Contracts/DPAs with cloud providers and sub-suppliers incorporating DV&P Addendum; sub-supplier register including locations and roles; mapping of DV&P controls to provider controls; assurance reports (ISO/SOC) for those services.	Must

38	Release Management	Configuration & Change Managemen	The core of the solution must not require custom code changes to meet the customer's functional requirements. Where customisation is necessary, it must be implemented outside the core (for example via configuration, extensions or add-ons) and managed through the supplier's change process, so that vendor upgrades and patches remain applicable.	Product architecture documentation (core vs extensions/customisation); customisation guidelines; change management procedure; examples of implemented customisations andTheirISOlation fromThe core; upgrade/patch records showing compatibility retained.	Must
39	Platform		The solution must be modular, so that functional sub-areas or components can be logically separated and replaced by alternative solutions with minimal impact on the remaining components. Interfaces and configuration must support this modularity.	Solution architecture with module/component boundaries and interfaces; documentation showing how modules can be disabled or replaced; examples (if available) of replacing or decoupling modules in similar environments; integration documentation.	Should
40	Release Management	Configuration & Change Managemen	The supplier must provide separate Development, Test, Acceptance and Production (DTAP) environments for the solution, with appropriate segregation of duties and data, and must implement a controlled promotion process between these environments.	Environment overview (DTAP), including segregation policy; SSDLC documentation; change/release management procedures showing promotion between DTAP; examples of recent changes with evidence of deployment path (Dev→Test→Acc→Prod).	Must
41	Platform	Supplier / Cloud Security	Any IaaS or PaaS components used for the solution must have documented backup, recovery, encryption, access control and continuity arrangements, and must be treated as sub-suppliers with documented locations and responsibilities.	Cloud architecture diagrams; mapping of IaaS/PaaS services to DV&P controls; CNAP compliance statement or checklist; sub-supplier register including locations and roles; backup/recovery and encryption configurations.	Must
42	Release Management	Configuration & Change Managemen	The solution must provide configuration capabilities that allow authorised administrators to implement functional changes (for example workflows, forms, business rules) without vendor code changes. Such changes must follow a documented change management process and must be protected by role-based access controls.	Configuration handbook; overview of configuration options vs. code changes; access control configuration for admin roles; change records showing functional changes executed by Enexis without vendor code changes; SSDLC/change procedure.	Must
43	Performance		Under normal operating conditions, the time to open the solution after successful authentication (initial load) must be ≤5 seconds for at least 95% of measurements, measured from completion of login to a fully rendered and usable landing page.	Performance test plan specifying "initial load" scenario and workloads; performance test reports with 95th percentile initial load ≤ 5 seconds; APM/monitoring data from production showing compliance forThe Enexis service.	Must
44	Performance		Under normal operating conditions, the response time for opening standard application screens must be ≤2 seconds for at least 95%, measured from the user's navigation action (for example menu or button click) until the screen is fully rendered and usable for key user journeys.	List of key user journeys/screens; performance test scripts and results showing 95th percentile ≤ 2 seconds; acceptance criteria and sign-off records; APM or monitoring reports from production demonstrating performance adherence.	Must
45	Reporting & Analysis		All end-user screens of the solution must be available in Dutch for the agreed user roles, including labels, menus, messages and help texts. Language files/resources must be maintained under version control and verified during each release.	Language/translation configuration (resource files); screenshots of main end-user screens in Dutch; release/test procedures including language verification; issue logs for language related defects and their resolution.	Must
46	Support		The supplier must provide first-line support to users in Dutch during the agreed service hours (at least normal business hours CET). First-line staff must be trained in the use of the solution and its security and privacy requirements, and the support model and language coverage must be documented in the SLA or support agreement.	Support model description (including languages per support tier); CVs or role profiles of 1st-line agents; training materials for support staff; sample tickets handled in Dutch; SLA specifying language and coverage times.	Must
47	Support	Security & Privacy	The supplier must be able to provide second-line and third-line support for the solution, preferably in Dutch (as a minimum in English), with personnel trained in the solution's technical architecture and security controls and available within the response times defined in the SLA.	Support organisation chart; description of 2nd/3rd line responsibilities; language capabilities of 2nd/3rd line staff; training records; SLA including response and resolution times for 2nd/3rd line escalations.	Should
48	Support	Incident Management	The supplier must be able to provide on workdays during working hours 7:00 - 18:00 support for incidents affecting the service, including on-call arrangements and escalation procedures, ensuring that high-priority incidents reported outside business hours meet the agreed response and repair times.	Incident management and escalation procedures; on-call rota for on workdays during working hours 7:00 - 18:00 support; SLA specifying on workdays during working hours 7:00 - 18:00 coverage for critical incidents; examples of incidents handled outside business hours with timestamps and resolutions.	Must
49	Support	Security & Privacy	The supplier must provide user and administrator documentation for the solution, including at least functional descriptions, step-by-step procedures, security and privacy-relevant user instructions, and troubleshooting guidance. Documentation must be kept up to date with each release.	User and admin manuals (PDF, online help, knowledge base); documentation version history; release notes referencing documentation updates; accessibility of documentation for Enexis users (URLs/portals).	Must
50	Security & Privacy	Privacy & Data Protection	All processing and storage of personal data related to the service (including support and administration) must take place exclusively within the EEA or in countries with an EU adequacy decision. The supplier must inform the customer and update the list of processing locations within one month of any change.	Filled-in and signed Appendix 3 – Locaties Informatie listing all processing locations; statement from supplier on data location policy; DPIA/TIA where applicable; change records showing timely updates to Appendix 3 after location changes.	Must
51	Security & Privacy	Privacy & Data Protection	The supplier must ensure that customer data, including personal data, is processed only for the purposes explicitly agreed in the contract and any data processing agreement, and is not shared or sold to third parties unless explicitly approved in writing by the customer and consistent with data protection law.	Signed Master Agreement and DV&P Addendum including data use clauses; Data Processing Agreement specifying purposes and prohibition on onward sale; data processing register showing purposes; supplier statement on no selling/sharing of Enexis data.	Must
52	Security & Privacy	Cryptography	The supplier must have and use documented key management processes for all encryption keys used for the service. These processes must cover, at a minimum: secure key generation, storage and distribution, role-based access to keys, regular key rotation and replacement, secure revocation and destruction of keys, and logging and review of key management activities.	Cryptography and key management policy; procedures for key lifecycle management; configuration and screenshots from key management systems (KMS/HSM); sample key rotation and access logs relevant to Enexis data.	Must
53	Security & Privacy	Cryptography	All customer data in storage for the solution (including databases, file storage, backups and archives) must be encrypted using industry-accepted algorithms with no known vulnerabilities, with encryption appropriate to the sensitivity of the data.	Technical documentation showing encryption at rest for databases, file systems and backups; configuration evidencing algorithms and key lengths; key management evidence (see ID 52); results of independent security assessments or audits.	Must
54	Security & Privacy	Cryptography	All data in transit between clients, services and integrated systems that involve customer data must be protected using strong, up-to-date cryptographic protocols (for example TLS 1.2 or higher) and secure configurations (no weak ciphers, no deprecated protocols). Mutual authentication must be used where required. Anonymous cipher suites and NULL ciphers must be disabled on all externally and internally exposed endpoints of the service.	Network/security architecture; TLS configuration (protocols, cipher suites); results from vulnerability scans/SSL tests; documentation of secure integration channels (e.g. VPN, MTLS) used for communication involving Enexis data.	Must
55	Security & Privacy	Application & API Security	The solution's network and application security must at least include: (1) a documented security architecture	Security architecture documentation; security control design and test results; logging configuration showing audit trail coverage; configuration evidence for account lockout (thresholds, duration); security test or penetration test reports.	Must
56	Security & Privacy	Application & API Security	The supplier must design and implement an application architecture that includes web security controls (such as authentication, authorisation, input validation, CSRF protection) and mechanisms to protect databases (such as least privilege, parameterised queries, encryption and segregation).	Application and database architecture diagrams; secure design documentation; database security configuration (roles, privileges, encryption); secure coding guidelines; security test reports focusing on web and database controls.	Must
57	Security & Privacy	Application & API Security	The supplier must implement application security controls in the software development process, including defined security requirements, secure coding guidelines, security code reviews and security testing (e.g. SAST and DAST) based on recognised standards such as OWASP Top 10 and relevant national web security guidelines.	SSDLC documentation; secure coding guidelines referencing OWASP/NCSC; examples of code review checklists and reports; results of SAST/DAST tools and tracking of remediation for identified vulnerabilities.	Must
58	Security & Privacy	Incident Management	The supplier must inform the customer immediately, and in any case within 4 hours of detection, of potential security vulnerabilities or personal data breaches affecting customer data, systems or services. The initial notification must include at least a preliminary impact assessment, measures taken and planned follow-up.	Incident response policy/procedure; notification templates; anonymised examples of security incident notifications sent to customers; records showing notification times vs detection times for relevant incidents.	Must
59	Security & Privacy	Incident Management	The supplier must have documented and implemented processes for information security incident management and crisis management that cover the services provided, including roles, responsibilities, escalation paths, communication with the customer and, where applicable, authorities, and integration with continuity and disaster recovery plans.	Incident and crisis management procedures; RACI or role descriptions; evidence of training or exercises (e.g. crisis simulations); examples of handled incidents/crises and corresponding reports; linkage to BCP/DRP documentation.	Must
60	Security & Privacy	Supplier / Cloud Security	The customer must have the right to audit the supplier and relevant sub-suppliers for the agreed services and/or the supplier must provide an independent assurance report annually (e.g. ISAE 3402 type 2, ISO 27001 audit report or SOC1/SOC2) covering the services and the agreed security and privacy requirements, including remediation of findings.	Contracts including audit clauses referencing The DV&P Addendum; latest ISO/SOC/ISAE reports with scope including Enexis services; management responses and remediation plans for findings; schedule of recurring assurance reporting to Enexis.	Must
61	Security & Privacy	Vulnerability & Patch Management	The supplier must allow the customer to perform penetration tests on the in-scope solution and/or demonstrate that independent penetration tests are carried out at least annually by qualified parties. Full, unredacted reports must be shared within two weeks after completion, together with documented remediation plans for identified findings.	Penetration test policy; latest independent pentest reports (scope including Enexis services); remediation plans and status for identified issues; agreements or procedures allowing Enexis to conduct its own pentests.	Must
62	Security & Privacy	Logging & Monitoring	The supplier must use security monitoring for systems, applications, networks, users and security components that are part of the service, including intrusion prevention, threat intelligence monitoring/hunting and vulnerability management, and must be able to provide summaries of relevant security events and trends on request.	Security monitoring and SIEM architecture; list of monitored components and data sources; sample security monitoring dashboards/reports; procedures for threat hunting and vulnerability handling; evidence of regular vulnerability scans.	Must
63	Security & Privacy	Supplier / Cloud Security	The supplier's organisation must operate an Information Security Management System (ISMS) and risk management framework in line with ISO 27001 or an equivalent standard, covering the services delivered. The ISMS must include documented risk assessments, treatment plans and regular management reviews.	ISO 27001 certificate and Statement of Applicability; ISMS scope including Enexis services; recent risk assessment and treatment plan; minutes of management reviews; internal or external audit reports referencingThe ISMS.	Must
64	Security & Privacy	Supplier / Cloud Security	The service and/or the supplier organisation providing the service must be independently certified to ISO 27001 (or equivalent) by an accredited certification body, with a scope that includes the relevant services, and the results must be shared annually or on request.	Valid ISO 27001 certificate, including scope statement; latest external audit report; accreditation information of The certification body; mapping of The certificate scope to The Enexis services.	Must
65	Security & Privacy	Security & Privacy	The supplier must apply recognised security standards and best practices relevant to the solution (for example Cloud Controls Matrix, OWASP, NIST, SOGP or equivalent), and must document which standards are applied, how they are implemented, and how compliance with these standards is periodically assessed.	Security policy and standards register; references in SSDLC and operations processes to specific frameworks (OWASP, NIST,CCM, etc.); results of internal or external assessments againstThese standards; remediation plans for identified gaps.	Should
66	Security & Privacy	Configuration & Change Managemen	The supplier must ensure that all changes to the service (including software, configuration, infrastructure and procedures) are assessed for their impact on information security and privacy, documented in the change record, and communicated in advance to the customer for changes that could affect the customer's risk profile.	Change management procedure including security/privacy impact assessment; sample change records showing documented impact, approvals and communication to Enexis; CAB minutes or change advisory approvals for significant changes.	Must
67	Security & Privacy	Logging & Monitoring	The solution must log user actions relevant to the customer (such as login/logoff, data creation, modification, deletion, administrative changes and data exports) in a way that makes it possible to reconstruct who did what, when and on which data. Logs must be protected against unauthorised access and modification and retained for at least the agreed retention period.	Logging design and configuration; examples of user activity logs showing required fields; log retention configuration; evidence of protection against tampering (e.g. append-only, hashing); procedures for providing logs to Enexis on request.	Must
68	Security & Privacy	Identity & Access Management	The solution must support configuration of multiple security policies (for example role-based access profiles, data visibility rules, retention/anonymisation rules) so that different policies can be applied for different user groups and data classifications.	Access control model and configuration options; examples of different security policies applied to roles or groups; documentation mapping BIVP/data classification to implemented policies; test cases showing enforcement of different policies.	Must
69	Security & Privacy	Network & Infrastructure Security	If the solution uses an interface with Microsoft Exchange Online (for example for calendar or email integration), the supplier must ensure that only modern, secure authentication methods are used (Microsoft Graph API with OAuth 2.0 or OIDC and that access is limited to the minimum permissions required for the agreed purposes.	Technical design for Exchange Online integration; configuration evidence showing use of modern authentication (OAuth 2.0, Graph API) and no legacy/basic auth; permission consent screens; security assessment or approval from Enexis.	Must
70	Support		The supplier must maintain and provide up-to-date operational documentation for the solution (including architecture, operations manuals, runbooks, backup and recovery procedures, and support processes) that is sufficient to operate, maintain and restore the service in line with agreed continuity objectives.	Operations manuals and runbooks; architecture and design documents; backup/restore procedures; evidence of periodic reviews/updates (version history); records of training or handover sessions usingThe documentation.	Must
71	Support		The supplier must provide up-to-date training documentation for the solution (e.g. user guides, e-learning, onboarding materials) to support the customer's security and privacy awareness programme and to ensure that relevant users and administrators can be trained at onboarding and at least annually.	Training documentation (user training guides, presentations, e-learning modules); version history of training materials; training plan showing use of These materials for Enexis staff; attendance/completion reports where training is delivered by The supplier.	Must
72	Platform	Configuration & Change Managemen	The supplier must provide and maintain technical system documentation for the solution, including architecture diagrams, interface specifications, configuration standards and technical runbooks, sufficient for the customer (or a designated third party) to understand, operate and restore the service in line with continuity requirements.	Technical design and architecture documents; interface specifications; configuration standards; operations runbooks; review log or version history showing regular updates; use of this documentation in DR/restore tests or handovers.	Must
73	Performance		The supplier must provide user and end-user help documentation for the solution (for example online help, manuals, FAQs, knowledge base), covering the main functions and security and privacy-relevant user instructions, and must keep this documentation aligned with each release.	User help manuals (PDF/online), FAQs, knowledge base articles; documentation version history; reference to documentation updates in release notes; accessibility of documentation for Enexis users (URLs/portals).	Must
74	Performance		The application must only be accessible to authorised identities by enforcing authentication via identity providers approved by the customer and access control policies based on least privilege and need-to-know. All accounts must be linked to identifiable individuals and managed through a formal registration and de-registration process.	Access control policy; integration design with Enexis IAM (idP/SSO); account lifecycle procedures (joiner/mover/leaver); user/account listings showing linkage to individuals; periodic access review reports for Enexis-related roles and systems.	Must
75	Support		The application must support single sign-on (SSO) for users using at least one of the following standards: OpenID Connect (OIDC), SAML 2.0 or domain join (domain join only for non-SaaS scenarios). SSO must be integrated with the customer's central identity provider(s).	SSO integration design; configuration showing use of OpenID Connect, SAML 2.0 or domain join; test reports for SSO login flows; documentation of trust relationships with Enexis IdP(s); screenshots/logs of successful SSO authentication.	Must
76	Support		For customer users, single sign-on via the approved identity provider must be the only interactive login method to the application (no local or alternative login mechanisms).	Configuration overview showing enabled authentication methods (only SSO); documentation or screenshots showing local/password login disabled; security test or penetration test results confirmingABsence of alternative login paths.	Must

77	Support		If SAML is used for SSO, the supplier must configure automatic certificate roll-over by regularly retrieving and applying updated metadata from the identity provider, and must handle changes to SAML metadata and certificates through the change management process.	SAML configuration screenshots (metadata URL, auto-update settings); change management records for past SAML certificate updates; test evidence for successful SAML authentication after certificate roll-over.	Should
78	Support	Incident Management	The application must use the customer's central account store(s) for authentication (for example AD/AAD/IdP), so that no separate identity store is used for authentication and all lifecycle events (joiner/mover/leaver) are centrally controlled.	Technical design describing use of Enexis central IdP/AD; configuration showing Enexis directory as authority for authentication; user account listings demonstrating identities are sourced from Enexis directories; JML procedures referencing Enexis IAM.	Must
79	Support		If the application maintains its own internal account store for authorisation (roles and permissions), it must support integration using SCIM v2 or an equivalent standard API for automated provisioning, de-provisioning and updating of accounts and role assignments based on the customer's central IAM systems.	API documentation for SCIM v2 or equivalent provisioning API; examples of provisioning/de-provisioning calls; test results for automated provisioning flows; configuration showing mapping between Enexis IAM attributes and application accounts.	Must
80	Identity & Access Management	Identity & Access Management	No local user accounts may be created or changed directly in the application for customer users. All user accounts and their authorisations must be provisioned, updated and revoked via central directories and/or provisioning interfaces. All access must be strictly personal and traceable.	User account management policy; configuration that disables or restricts local user management; audit of current accounts showing origin (provisioned vs local); sample de-provisioning records demonstrating automatic removal after employment end/role change.	Must
81	Identity & Access Management	Identity & Access Management	The application must implement role-based access control, where access rights are granted through roles defined in agreement with the customer. Role-to-identity mappings must be managed centrally and the permissions associated with each role must be managed within the application and documented in an authorisation matrix.	Access control/authorisation model; role and permission matrix; configuration screens showing role assignment and permissions; examples of role assignments provisioned from Enexis IAM; periodic access review reports for Enexis roles.	Must
82	Identity & Access Management	Identity & Access Management	When identities are exposed outside the customer's environment (for example to cloud services or sub-suppliers), the supplier must ensure that only the minimal set of personal attributes required for the requested functionality is transferred and processed, and must keep the list of such processing locations up to date.	Data flow diagrams showing which identity attributes are shared and with which parties; attribute minimisation design; filled-in and updated Appendix 3 – Locaties Informatie; RoPA entries covering identity data transfers and purposes.	Must
83	Identity & Access Management	Identity & Access Management	The solution must comply with applicable Dutch and European privacy laws and regulations (including GDPR/AVG) for all processing of personal data, including lawful basis, purpose limitation, data minimisation, transparency, data subject rights, security of processing, international transfers and retention/deletion obligations.	Signed DPA andDV&P Addendum; Records of Processing Activities (RoPA) for Enexis data; DPIA where required; technical and organisational measures overview; evidence of processes for data subject rights, retention/deletion, and data transfer controls.	Must
84	Identity & Access Management	Identity & Access Management	If the solution contains AI or machine-learning capabilities, the supplier must provide and maintain a complete overview of all AI functions used for the service, including for each function at least: purpose, input data categories, output types, whether personal or confidential data are processed and in which environments the function is enabled.	AI/ML functionality inventory forThe Enexis service; documentation describing per AI function: purpose, input/output, data categories and environments; change records showing updates ofThis overview after new AI features are introduced.	Must
85	Identity & Access Management	Identity & Access Management	AI capabilities in the solution must not send confidential or personal customer data to external AI or model providers or platforms by default. Such transfers may only occur after explicit technical configuration and prior written approval by the customer.	Technical design showing AI integrations and data flows; configuration screenshots showing external AI endpoints disabled by default; written approvals from Enexis for any enabled external AI data transfer; updated DPA and Appendix 3 coveringThese transfers.	Should
86	Identity & Access Management	Identity & Access Management	The solution must ensure that AI-generated content is clearly distinguishable from user-generated content, for example through visual labels, dedicated fields or metadata flags, so that users can recognise AI-generated output.	Configuration documentation for AI features; administration screens showing enable/disable and scoping options for AI per environment/role; examples of configuration where AI is disabled or limited for specific user groups inThe Enexis tenant.	Must
87	Identity & Access Management	Identity & Access Management	The solution must provide configuration options that allow authorised administrators to centrally disable or restrict AI features that process or generate content based on customer data, at least per environment and per user group or role.	AI model documentation or factsheets; internal risk/impact assessments for AI models; copies of documentation shared with Enexis describing training data sources and limitations; review records at Enexis side.	Must
88	Security & Privacy	Privacy & Data Protection	The supplier must document the main training data sources/categories and known limitations (such as biases, accuracy ranges, unsupported languages or domains) of the AI models used in the service, and must make this information available on request.	Signed approvals from Enexis for AI training/fine-tuning; specific DPA/addendum describing AI training use; records of training datasets showing scoping to agreed data; DPIA/TIA where personal data is involved.	Must
89	Security & Privacy	Privacy & Data Protection	Customer-specific data may only be used to train or fine-tune AI models after explicit written approval by the customer and under a separate data processing and confidentiality agreement specifying purposes, data categories, locations and retention periods.	Access control model showing AI-related permissions; configuration examples where AI access is restricted to certain roles; test users demonstrating that AI functions are only available to authorised roles; access review reports including AI-specific permissions.	Must
90	Security & Privacy	AI Security & Governance	The solution must support role-based access control specifically for AI features, so that the customer can restrict which users and service accounts may invoke AI models or access AI-generated insights.	Logging design for AI components; sample AI prompt logs with required fields and pseudonymisation/anonymisation options; configuration options for masking/suppressing sensitive fields; procedures for providingSuch logs to Enexis upon request.	Must
91	Security & Privacy	AI Security & Governance	Prompts and inputs sent to AI components that contain customer data must be logged in a secure manner for audit and incident investigation, including at least timestamp, calling identity and AI function. The solution must offer options to limit or pseudonymise logged sensitive content.	AI risk assessment or threat model documents; review schedule showing at least annual updates; records of actions taken to mitigate identified AI risks; linkage of AI risk assessment toThe overall ISMS risk register.	Must
92	Security & Privacy	AI Security & Governance	The supplier must perform and document a risk assessment specifically for the AI capabilities used in the service, covering at least misuse, model errors, data leakage and bias, and must update this assessment at least annually or after major AI-related changes.	Technical architecture showing write-back paths for AI; configuration options enforcing human-in-the-loop or approval workflows; sample workflows demonstrating required approvals before AI-initiated changes are committed; risk analysis for such write-backs.	Must
93	Security & Privacy	AI Security & Governance	The solution must provide configuration options to prevent AI components from writing back directly to authoritative data sources (for example ERP or asset management systems) without explicit workflow approval or human review where the action can materially impact operations or safety.	ISO/SOC certificates and scope statements explicitly mentioning AI services or platforms; mapping of AI components toThe certified scope; latest assurance reports including controls relevant for AI environments; supplier statement confirming coverage.	Should
94	Security & Privacy	AI Security & Governance	For SaaS solutions, the AI models and their hosting environments that process customer data must be covered by the same security controls and independent certifications (for example ISO 27001, SOC2) as the rest of the application and platform. Evidence of this must be provided on request.	Configuration documentation and screenshots showing toggle for training/model improvement on/off; default settings for Enexis tenants; DPA or contractual clauses governing use of Enexis data for training; logs or statements showing no retention when disabled.	Must
95	Security & Privacy	AI Security & Governance	The solution must provide configuration options to ensure that AI features do not retain or reuse customer prompts and outputs for model improvement or training, unless the customer has explicitly agreed to such use in writing.	DPIA support documentation (questionnaires, technical annexes); completed DPIA templates where available; data flow diagrams for AI processes; evidence of cooperation with Enexis privacy officers during DPIA activities.	Must
96	Security & Privacy	AI Security & Governance	The solution must support role-based access control specifically for AI features, so that the customer can restrict which users and service accounts may invoke AI models or access AI-generated insights.	Logging design for AI components; sample AI prompt logs with required fields and pseudonymisation/anonymisation options; configuration options for masking/suppressing sensitive fields; procedures for providingSuch logs to Enexis upon request.	Should
97	Security & Privacy	AI Security & Governance	Prompts and inputs sent to AI components that contain customer data must be logged in a secure manner for audit and incident investigation, including at least timestamp, calling identity and AI function. The solution must offer options to limit or pseudonymise logged sensitive content.	AI risk assessment or threat model documents; review schedule showing at least annual updates; records of actions taken to mitigate identified AI risks; linkage of AI risk assessment toThe overall ISMS risk register.	Must
98	Security & Privacy	AI Security & Governance	The supplier must perform and document a risk assessment specifically for the AI capabilities used in the service, covering at least misuse, model errors, data leakage and bias, and must update this assessment at least annually or after major AI-related changes.	Technical architecture showing write-back paths for AI; configuration options enforcing human-in-the-loop or approval workflows; sample workflows demonstrating required approvals before AI-initiated changes are committed; risk analysis for such write-backs.	Must
99	Security & Privacy	AI Security & Governance	The solution must provide configuration options to prevent AI components from writing back directly to authoritative data sources (for example ERP or asset management systems) without explicit workflow approval or human review where the action can materially impact operations or safety.	ISO/SOC certificates and scope statements explicitly mentioning AI services or platforms; mapping of AI components toThe certified scope; latest assurance reports including controls relevant for AI environments; supplier statement confirming coverage.	Must
100	Security & Privacy	AI Security & Governance	For SaaS solutions, the AI models and their hosting environments that process customer data must be covered by the same security controls and independent certifications (for example ISO 27001, SOC2) as the rest of the application and platform. Evidence of this must be provided on request.	Configuration documentation and screenshots showing toggle for training/model improvement on/off; default settings for Enexis tenants; DPA or contractual clauses governing use of Enexis data for training; logs or statements showing no retention when disabled.	Must
101	Security & Privacy	AI Security & Governance	The solution must provide configuration options to ensure that AI features do not retain or reuse customer prompts and outputs for model improvement or training, unless the customer has explicitly agreed to such use in writing.	DPIA support documentation (questionnaires, technical annexes); completed DPIA templates where available; data flow diagrams for AI processes; evidence of cooperation with Enexis privacy officers during DPIA activities.	Should
102	Security & Privacy	AI Security & Governance	For AI capabilities that process personal data, the supplier must support the customer in performing a Data Protection Impact Assessment (DPIA) or similar assessment by providing all necessary technical and organisational information about these AI functions, including data flows, recipients, retention and safeguards.	Secure design documentation for AI components; description of implemented controls against prompt injection and related attacks; security test reports (including targeted tests on AI prompts); SSDLC artefacts referencing AI-specific security measures.	Could
103	Security & Privacy	AI Security & Governance	Where AI capabilities such as large language models are used, the supplier must implement mechanisms to prevent prompt injection and similar AI-specific attacks (for example input validation, contextual separation of system and user prompts, output filtering), and must test these mechanisms as part of the development lifecycle.	Incident response procedure including AI-specific scenarios; training or exercises addressing AI incidents; examples (if any) of AI-related incidents and notifications; mapping between AI incident handling andThe general Enexis incident notification requirements.	Must
104	Security & Privacy	Cryptography - PQC	The application supports crypto-agility by allowing cryptographic algorithms, key sizes and protocol versions to be changed through configuration without requiring changes to the core application code.	Architecture and configuration documentation showing that cryptographic algorithms, key sizes and protocol versions are configurable without modifying core application code, examples of configuration changes where algorithms or protocol versions were updated, and associated test reports demonstrating correct operation after such changes.	Should
105	Security & Privacy	Cryptography - PQC	The application does not rely on hard-coded cryptographic algorithms, key sizes or protocol versions in a way that prevents migration to post-quantum-capable alternatives; these parameters are configurable.	Code and configuration review reports showing that cryptographic parameters are not hard-coded in a way that blocks migration, configuration guides explaining how to adjust algorithms, key sizes and protocol versions, and examples of successful cryptographic parameter changes without source code modifications.	Should
106	Security & Privacy	Cryptography - PQC	The application allows configuration of the cryptographic algorithms and key sizes used for TLS on all external interfaces, including web user interfaces, APIs and integration endpoints. For all outbound TLS connections initiated by the solution (e.g. to APIs, databases, mail relays), the supplier must enforce full certificate and certificate chain validation. Disabling certificate validation or accepting self-signed certificates is only allowed where explicitly configured for specific endpoints and approved by the customer in writing.	TLS configuration documentation for all external interfaces, evidence that algorithms and key sizes can be configured via settings or configuration files, and examples of TLS configuration changes with corresponding successful test results.	Should
107	Security & Privacy	Cryptography - PQC	The application supports TLS configurations that can be extended to use post-quantum or hybrid key exchange and authentication mechanisms when these are supported by the underlying platform and client software.	Architecture and platform documentation describing the TLS stack and its ability to support extended key exchange and authentication mechanisms, supplier statements or vendor documents confirming support for larger or hybrid cipher suites, and proof-of-concept or test results using such extended TLS configurations without functional failures.	Should
108	Security & Privacy	Cryptography - PQC	The application allows configuration of the cryptographic algorithms and key sizes used for data at rest, including databases, file storage and application-level encryption, so that encryption can be migrated to post-quantum-resistant alternatives.	Encryption configuration documentation for data at rest, showing how algorithms and key sizes can be selected and changed for databases, file storage and application-level encryption, together with examples or test results where stronger or different algorithms were configured and validated.	Should
109	Security & Privacy	Cryptography - PQC	The application supports re-encryption of stored data, including databases, file storage and backups, with new cryptographic algorithms and keys without requiring changes to the business logic of the application.	Documented procedures and tools for re-encrypting databases, file storage and backups, migration or test reports showing successful re-encryption with new algorithms and keys while preserving application functionality and data integrity, and rollback procedures in case of re-encryption issues.	Should
110	Security & Privacy	Cryptography - PQC	The application supports the use of multiple active key pairs and certificates per purpose, for example for TLS, SAML and code signing, so that classical and post-quantum or hybrid algorithms can be used in parallel during a migration.	Configuration documentation showing support for multiple active keys or certificates for each use case such as TLS, SAML and code signing, examples of environments where multiple key pairs or certificate types are configured and active at the same time, and test results for key roll-over and parallel use without service interruption.	Should
111	Security & Privacy	Cryptography - PQC	The application ensures that long-lived secrets, including master keys, roots of trust and long-term static keys, are not bound to a specific cryptographic algorithm in a way that prevents timely replacement by post-quantum-resistant alternatives.	Key management design documents describing how long-lived secrets are stored, referenced and rotated, evidence that secret identifiers and interfaces do not hard-bind secrets to a single algorithm, and examples or procedures showing replacement of long-lived keys with different algorithm types without major architectural changes.	Should
112	Security & Privacy	Cryptography - PQC	The application operates correctly in environments where certificate sizes, key sizes and handshake messages are larger than with current classical algorithms, without functional failures or protocol violations.	Performance and interoperability test results using larger certificates and key sizes, and larger TLS handshake messages, evidence that client and server components handle increased message sizes without protocol parsing errors, timeouts or connection failures, and any documented limits or tuning settings for message sizes.	Should
113	Security & Privacy	Cryptography - PQC	The application supports the use of external key management systems or hardware security modules to store and manage keys, in a way that does not restrict the use of post-quantum-capable key types when the underlying key management system supports them.	Integration documentation for external key management systems or hardware security modules, configuration examples showing use of external key stores for cryptographic operations, vendor or platform documentation confirming that new or post-quantum key types can be used when supported by the external system, and test or proof-of-concept results where applicable.	Should
114	Security & Privacy	Cryptography - PQC	The application provides mechanisms to switch cryptographic configurations per environment, such as development, test and production, to enable phased migration to post-quantum-capable algorithms.	Environment configuration documentation showing how cryptographic settings can differ between development, test and production, examples of environment-specific cryptographic configurations, and change records plus test reports demonstrating phased changes to cryptographic settings across environments.	Should
115	Security & Privacy	Cryptography - PQC	The application supports deployment in test and other non-production environments with alternative cryptographic configurations, including larger keys and experimental post-quantum or hybrid algorithms, without requiring code changes.	Deployment and configuration guides describing how alternative cryptographic configurations can be used in non-production environments, test reports from such environments using larger keys or experimental algorithms, and evidence that no application source code changes were required for these scenarios.	Should

116	Security & Privacy	Cryptography - PQC	The application supports rollback of cryptographic configuration changes, including algorithm and key changes, to a previous working configuration without corrupting encrypted data or breaking integrity checks.	Change and rollback procedures for cryptographic settings, examples of executed rollbacks where previous algorithms or keys were restored, and evidence that encrypted data remained readable and integrity checks remained valid after rollback.	Should
117	Security & Privacy	Cryptography - PQC	The application provides a machine-readable export or interface, such as configuration files or APIs, that describes its active cryptographic configuration so that Enexis can assess readiness for post-quantum migration.	Documentation of configuration export formats or APIs that list active cryptographic settings, sample exports or API responses showing current algorithms, key sizes and protocol versions, and a description of how this information is kept up to date with the running system.	Should
118	Security & Privacy	Cryptography - PQC	The application does not introduce proprietary cryptographic algorithms or formats that cannot be migrated to or co-exist with standardised post-quantum algorithms for encryption, key exchange or digital signatures.		Should
119	Release Management	Release Management / Platform	When implementing new releases, all previously implemented configurations and customer-specific functional settings of the solution must be preserved, so that no regression or loss of existing functionality occurs as a result of the upgrade.	Release and change management procedures; configuration management documentation (including parameter/config export); sample release notes and regression test reports showing preservation of existing configuration and functionality after upgrades.	Must
120	Release Management	Client & Device / Platform	The user solution must support the customer's "N" operating system strategy: for all major, commonly used client operating systems, the solution must support at least the current major release (N) and one previous major releases (N-1), and must document the list of supported OS versions and any exceptions.	Supplier support statement/matrix listing supported client operating systems and versions (including N, N-1, N-2); test reports (FAT/UAT) on representative customer workplace images; release policy documentation showing how new OS releases are onboarded and older versions are phased out.	Must
121	Security & Privacy	Governance & Policy	The supplier must operate a documented and approved Information Security and Privacy Policy, including clearly assigned roles and responsibilities, documented threat analysis and asset inventory, and a process for identifying applicable legal and contractual requirements. This policy and its implementation must be reviewed at least annually and after major changes, with documented outcomes and actions.	Information Security & Privacy Policy document; RACI or role descriptions; latest threat analysis and risk register; up-to-date asset/information inventory; register of applicable laws and contractual security requirements; management review minutes and follow-up actions.	Must
122	Security & Privacy	Supplier & Chain Management	The supplier must implement a structured supplier and ICT supplychain security process for all sub suppliers involved in delivering the service, including documented security and privacy requirements in contracts, regular performance and risk reviews (at least annually), and protection of intellectual property and compliance records relevant to the Enexis service.	Supplier and sub-supplier register (including roles and locations); template and signed contracts/DPAs with security & privacy clauses and IP provisions; records of periodic supplier risk/performance reviews and audits; examples of corrective actions based on these reviews; register of compliance evidence and certifications for key suppliers.	Must
123	Security & Privacy	Vulnerability & Patch Management	The supplier must operate a documented vulnerability and patch management process covering all components of the service, including at least monthly vulnerability scanning, documented riskbased prioritisation (e.g. CVSS), defined remediation timeframes per severity (e.g. critical within 14 days), tracking of remediation progress, and verification that patches and mitigations are successfully applied in all relevant environments.	Vulnerability management policy and process description; vulnerability scan schedules and reports; remediation tracking (tickets/change records) showing patch timelines vs. targets; examples of emergency patch handling for critical issues; reports or dashboards summarising vulnerability status for the Enexis service.	Must
124	Security & Privacy	Data Lifecycle & Media Handling	The supplier must define and implement data lifecycle and media handling processes for the service, including: (1) secure deletion or anonymisation of customer data and media when retention periods expire or on customer request, (2) documented handling and encryption requirements for all storage and removable media in line with data classification, and (3) controls to prevent unauthorised data leakage (e.g. restrictions and logging for mass exports and removable media).	Data lifecycle policy (retention, deletion/anonymisation rules); media handling procedures; configuration of encryption for storage and removable media; logs or evidence of executed data deletions/anonymisations; configuration or policy for restricting and logging exports and use of removable media; DPIA or data protection documentation describing these controls.	Must
125	Security & Privacy	Secure Development & Testing	The supplier must operate a secure software development and release process for the service, including: (1) documented security requirements and design reviews, (2) security testing (SAST, DAST and, where applicable, penetration testing) for each major release with defined acceptance criteria, (3) formal installation and change procedures for production systems (plan, impact analysis, approvals, fallback and documented tests), and (4) specific security clauses for outsourced development (including secure coding, test obligations, audit rights and escrow).	Secure SDLC policy and procedures; sample security requirements and design review records; security test plans and reports (SAST/DAST/pentest) per release; change records showing use of formal installation/change procedures; contracts with development partners including security clauses and audit/escrow provisions; examples of supplier audits or reviews.	Must
126	Security & Privacy	Availability & ICT Continuity	The supplier must align information security and ICT continuity for the service with defined business continuity objectives, by maintaining documented continuity requirements (including availability, RTO/RPO and capacity), implementing and testing technical and organisational measures such as redundancy and failover at least annually, and keeping evidence that these measures remain effective during adverse situations.	Business continuity and ICT continuity requirements for the Enexis service; architecture diagrams showing redundancy/failover for critical components; results of continuity/DR tests (including failover and capacity tests) against defined objectives; records of improvements based on test outcomes; capacity monitoring data demonstrating that agreed performance and availability targets are met.	Must
127	Security & Privacy	Identity & Access Management	For all privileged accounts and all remote administrative access to the solution, multi-factor authentication (MFA) must be enforced using the customer's central identity provider. MFA must be mandatory (no fallback to single-factor) and must be applied consistently across all administrative interfaces (e.g. web UI, APIs, management consoles).	Access control and authentication design; configuration screenshots/logs from IdP and application showing MFA enforcement for administrative roles; test evidence of login attempts without MFA being rejected; overview of privileged roles and confirmation that MFA is enabled for all.	Must
128	Security & Privacy	Logging & Monitoring	The solution must not log passwords, full authentication secrets, cryptographic keys, tokens or other highly sensitive secrets in plain text in any logs or monitoring outputs. Where such data is needed for troubleshooting, it must be masked, truncated or otherwise irreversibly protected.	Logging and error-handling design; examples of application and infrastructure logs for authentication and crypto operations; configuration or code snippets showing masking/truncation of sensitive fields; results from log reviews or security assessments confirming absence of plaintext secrets.	Must
129	Platform	Network & Infrastructure Security	The solution must support configuration options to disable or restrict access from the public internet, for example through IP allowlists, private endpoints, VPN only access or equivalent mechanisms, in accordance with the customer's network access policies.	Network design and configuration documentation; examples of IP allowlist/private endpoint/VPN-only configurations; screenshots or configuration exports from cloud/network platforms; test evidence showing that access is blocked when not from allowed networks.	Must
130	Platform	Supplier / Cloud Security	For SaaS solutions, the supplier must have DDoS protection in place for all externally accessible interfaces of the service and must be able to demonstrate how DDoS attacks are detected, mitigated and reported, including any impact on availability SLAs.	Cloud/platform design describing DDoS protection mechanisms; contracts or service descriptions from underlying cloud providers; example dashboards or incident reports of past DDoS events (anonymised); SLA or resilience documentation explicitly referencing DDoS protections	Must
131	Client & Device	Identity & Access Management / Lea	The solution must not require elevated local operating system permissions (such as local administrator or root) for normal end-user operation. Elevated permissions may only be needed for installation or maintenance by authorised administrators.	Workplace and installation documentation; system requirements stating required privileges; test reports showing successful operation under standard user accounts; evidence that only installation/maintenance tasks require elevated rights.	Must
132	AI	AI Governance	AI governance compatibility Route all AI traffic through the single Enexis control plane. There is exactly one AI Gateway (API, Docs) for generative AI traffic, exactly one MLOps platform for traditional ML, and exactly one AgentOps stack for agentic AI.	Documentation how the solution can integrate with the Enexis AI environment.	Should
133	AI	AI Governance	Human accountability A human is always accountable for the decisions an AI system supports or takes so it must be able to overrule AI Decisions and autonomy is earned not granted	Provide logging to show reasoning of AI and ability to audit its conclusions/decisions. Documentation on how human	Must
134	AI	AI Governance	AI Configuration An AI BOM must describe what products / models are used for the (embedded) AI Solution, where its data resides and that retention periods can be monitored	Provide a complete and current AI Bill of Materials (AIBOM) identifying all AI-related components including models, model versions, AI providers, agents, tools, MCP servers, connectors, orchestration frameworks, vector databases, knowledge sources, external AI services, and supporting infrastructure. Include data-flow diagrams, data residency documentation, retention configurations, and configuration exports demonstrating where data is processed, stored, retrieved, and retained. Provide auditable evidence that all components, data locations, retention settings, and dependencies can be monitored, versioned, and reviewed by Enexis.	Must
135	AI	AI Governance	AI ACT The vendor must comply to the EU AI ACT and support Enexis with needed documentation and evidence needed at audits and supervisory inquiries	Provide a complete AI Act compliance dossier, including AI risk classification, technical documentation, governance controls, testing and validation evidence, human oversight measures, incident management procedures, and auditable records. Demonstrate the ability to support Enexis during audits, regulatory inspections, supervisory inquiries, and conformity assessments, including evidence for all underlying models, agents, tools, MCP servers, connectors, and third-party AI services used in the solution.	Must