

Annex 8: Security in Development and Operations

This annex describes the Processor's measures for security in the development and operation of the platform. It supplements Annex 1 and is based on the Processor's internal policies on patch management and change management.

1. Patch and vulnerability management

1.1 Scope. Patch management covers, on a mandatory basis, all production-relevant components within the Processor's area of responsibility, in particular operating systems, container images, base images, container runtimes and orchestration platforms, in-house developed and third-party standard software, third-party libraries, frameworks, packages and runtime dependencies in use, database servers and engines, infrastructure components, and security components including firewalls, endpoint security, identity and single sign-on components, scanners, and monitoring and security tools.

For services operated entirely by external providers, patch management for the underlying platform rests with the respective provider. The Processor remains responsible for patching its own configurations and workloads, for updating its own applications and deployments, for evaluating provider-side security advisories, and for the risk assessment and tracking of relevant security updates.

1.2 Identification. Security and functional updates are identified on an ongoing basis through vendor information, security advisories, internal findings, monitoring, support cases and other technical indications.

1.3 Assessment and prioritisation. Each relevant patch is assessed with regard to the criticality of the vulnerability, the extent to which the platform is affected, the impact on data protection and information security, operational and availability risks, and compatibility with existing components. Prioritisation is carried out by technical management.

1.4 Remediation deadlines. Security-relevant updates are implemented according to priority within the following deadlines:

Category	Remediation deadline
Critical security updates: immediate and substantial threat to confidentiality, integrity or availability, or active exploitation	without undue delay

Category**Remediation deadline**

High priority: high risk, exploitation likely or substantial operational impairment possible

within 24 hours

Medium priority: relevant but not immediate risk

within 2 days

Low priority: limited security relevance

within 3 days where required for security reasons,
otherwise in the regular release cycle

1.5 Approval. Production patch measures are approved by technical management under the four-eyes principle. Critical security updates may be implemented outside regular release cycles.

1.6 Exceeded deadlines. Where a patch cannot be implemented within the applicable deadline, technical management decides on the further course of action. The reasons for the delay and any compensating measures taken are documented in a traceable manner. Compensating measures include in particular configuration adjustments, deactivation of functions that are not required, access restrictions, additional monitoring measures and organisational restrictions until the patch is implemented.

2. Security in development and change management

2.1 Scope. All production-relevant changes are covered, in particular changes to backend and frontend components, infrastructure and cloud components, databases and storage components, security and configuration components, integrations and interfaces to third-party systems, as well as deployments, releases and configuration changes.

2.2 Principles. Every production-relevant change is documented and versioned before implementation and logged in a traceable manner after implementation. Changes are assessed before implementation with regard to their impact on security, data protection, availability and functionality, and are tested before being released into the production environment. Development, test and production environments are kept separate.

2.3 Versioning and documentation. Git is the mandatory standard for source code versioning. Every production-relevant change is centrally documented, stating the description and objective, the systems affected, the risk assessment, the testing approach, the approval, the time of implementation and, where applicable, rollback information.

2.4 Approval. Production changes are approved by technical management under the four-eyes principle.

2.5 Testing before go-live. Two manual functional tests are mandatory, one performed by a developer and one by an independent tester, together with automated end-to-end tests for central processes, in particular account creation, login, onboarding, calendar integration and account deletion. For critical or production-relevant changes, these are supplemented by smoke tests of the core functions, targeted testing of the affected components and interfaces, regression tests for known critical functions, and evaluation of relevant logs and monitoring alerts following deployment.

2.6 Verification after go-live. Following implementation it is verified that the affected functions operate correctly, that no obvious consequential errors occur, that the platform remains stable and available, and that no security- or data-protection-relevant malfunctions are apparent.

2.7 Rollback. For production changes it is possible to revert to a previous stable state. All relevant artefacts are retained and the platform is operated on a container basis.

2.8 Emergency changes. An accelerated process applies to critical security incidents, serious errors and acute production disruptions outside the regular release cycle. The principle of controlled implementation applies in these cases as well; full documentation, subsequent review and confirmation of approval follow without undue delay.

3. Evidence and retention

Manual reviews are documented in the respective pull request by the responsible tester; the pull request is approved only after successful review and only then merged. Automated reviews are documented in the deployment pipelines and retained there in a traceable manner.

The documentation covers at minimum the component affected, the trigger and source, the priority, the date of assessment and of implementation, the responsible roles, the test results, and any deviations and compensating measures.

Patch- and change-related artefacts and evidence are retained for at least one year.

4. Security testing

The Processor has the platform subjected to a penetration test by an independent third party at regular intervals, at least annually. Vulnerabilities identified are remediated in accordance with the deadlines set out in section 1.4. A summary of the results is made available to the Controller on request.

5. Periodic review

The patch and change management processes are reviewed regularly for effectiveness, currency and appropriateness and are adjusted where necessary. This applies in particular where the system architecture changes, where new regulatory requirements arise, or where the threat landscape changes.