Allegra

Dokument

Projekthandbuch

	Name	Datum	Unterschrift
Ersteller:	Freeman, Chris	21.08.2019 22:34	
Bearbeiter:	Freeman, Chris	-	
Manager:	Freeman, Chris	-	
Letzte Änderung: 21.08.2019 22:34		Seite 1 von 30	Exportdatum: 06.11.2024 17:18
Letzter Bearbeiter: Freeman, Chris			Projekthandbuch
Ersteller: Freeman, Chris		Dok.-Nr.: 1295	Alltena GmbH

Inhaltsverzeichnis

1. Einleitung

Das V-Modell ist ein generischer Vorgehensstandard, der für unser Projekt angepasst und konkretisiert werden muss. Dieses Projekthandbuch legt die notwendigen Anpassungen und Ausgestaltungen fest ("Tailoring"). Es beschreibt sozusagen unseren projektspezifischen Prozess.

Wenn Du noch nie mit dem V-Modell zu tun hattest: „Produkte“ bedeutet darin alles, was im Rahmen eines Vorhabens produziert wird, also nicht nur das Endprodukt, sondern auch alle Arten von Dokumenten und Zwischenergebnissen.

Das Projekthandbuch beinhaltet

- eine Kurzbeschreibung des Projekts
- die Beschreibung des Tailoring-Ergebnisses. Dazu gehören als wesentliche Bestandteile eine Liste mit den Typen der zu erstellenden Produkte sowie eine Beschreibung der Rollen
- den grundlegenden Projektdurchführungsplan
- die notwendige und vereinbarte Unterstützung des Auftraggebers
- Organisation und Vorgaben für die Planung und Durchführung des Projekts und die anstehenden Entwicklungsaufgaben.

Dazu gehören z.B. eine Liste der einzusetzen-den Werkzeuge, Programmiersprachen und Rahmenwerke. Der Projektleiter muss dieses zentrale Produkt in Abstimmung mit den Schlüsselpersonen des Projekts erarbeiten.

Im Projekthandbuch werden auch Häufigkeit und Notwendigkeit der Erzeugung weiterführen-der Produkte, die für die Planung und Durchführung des Projekts, für das Ausschreibungs- und Vertragswesen sowie für die Prozessverbesserung notwendig sind, festgelegt, zum Beispiel Projektstatusberichte, Risikolisten, Verträge und Bewertungen von Vorgehensmodellen.

Hinweis an den Projektleiter: Gehe alle Punkte in diesem Dokument durch. Wenn Du auch nach längerer Überlegung keine Idee hast, wozu ein Abschnitt in Deinem Vorhaben gut sein soll, lass ihn weg! Schlimmer als etwas zu viel wegzulassen ist etwas hinzuschreiben, ohne den Nutzen zu sehen.

2. Projektüberblick, Projektziele und Erfolgsfaktoren

Das Projekthandbuch ist eine unverzichtbare Informationsquelle und Richtlinie für alle Projektbeteiligten. In diesem Abschnitt wird kurz, prägnant und möglichst plastisch das gemeinsame Projektleitbild dargestellt.

3. Projektspezifisches V-Modell

3.1 Projekttyp

Systementwicklungsprojekt (AG/AN)

3.2 Projekttypvariante

AG-AN-Projekt mit Entwicklung, Weiterentwicklung oder Migration

3.3 Anwendungsprofil

Kaufmännisches Projektmanagement	nein
Messung und Analyse	nein
Informationssicherheit und Datenschutz (AG/AN)	ja
Funktionssicherheit (AG/AN)	ja
Projektgegenstand	HW und SW
Unterauftrag	nein
Prototypentwicklung	ja
Fertigprodukte	ja
Benutzerschnittstelle	ja
Altsystem	nein
Betriebsübergabe (AG/AN)	nein

3.4 Ausgewählte Vorgehensbausteine

Die folgenden Bausteine sind zwingend erforderlich, wenn Hardware und Software zu liefern sind. Sonst kann man einen der beiden Bausteine weglassen.

Projektmanagement	
Qualitätssicherung	
Konfigurationsmanagement	
Problem- und Änderungsmanagement	
Anforderungsfestlegung	
Systemerstellung	
HW-Entwicklung	
SW-Entwicklung	
Lieferung und Abnahme (AG)	
Lieferung und Abnahme (AN)	

Die folgenden Bausteine sind optional, je nach Art des Projektes.

Kaufmännisches Projektmanagement	
Messung und Analyse	
Informationssicherheit und Datenschutz	
Informationssicherheit und Datenschutz (AG)	
Informationssicherheit und Datenschutz (AN)	
Funktionssicherheit	
Funktionssicherheit (AG)	
Funktionssicherheit (AN)	
Logistikkonzeption	
Evaluierung von Fertigprodukten	
Benutzbarkeit und Ergonomie	
Betriebsübergabe	
Betriebsübergabe (AG)	
Betriebsübergabe (AN)	
Vertragsschluss (AG)	
Weiterentwicklung und Migration von Altsystemen	

4. Abweichungen vom V-Modell

Sämtliche Abweichungen von den Vorgaben des V-Modells, wie Streichungen einzelner Produkte, Aktivitäten und Abweichung vom Tailoring-Verfahren, müssen unter Angabe von Grün-den dokumentiert werden. Die Änderungen sind in diesem Abschnitt aufzuführen.

5. Projektdurchführungsplan

Das V-Modell macht durch die Festlegung von Entscheidungspunkten Vorgaben zur groben Strukturierung des Projekts. Dieser Abschnitt enthält die planerische Ausgestaltung dieser Entscheidungspunkte in Form eines Projektdurchführungsplans. Hierbei sind zumindest der Projektanfang, das Projektende und alle wichtigen Entscheidungspunkte während des Projekts einzuplanen. Es muss dokumentiert werden, welche Produkte für das Herbeiführen ei-ner Projektfortschrittsentscheidung, also dem Erreichen eines Entscheidungspunktes erforderlich sind.

Darüber hinaus können noch weitere projektspezifische Meilensteine festgelegt werden, so-weit diese für alle Projektbeteiligten relevant sind. Meilensteine, die nur projektintern relevant sind, werden im Projektplan dokumentiert.

6. Organisation und Vorgaben zum Projektmanagement

In diesem Abschnitt werden die Vorgaben des V-Modells zum Projektmanagement angepasst und konkretisiert. Es werden alle internen und externen Projektbeteiligten aufgeführt. Die verantwortlichen Ansprechpartner sind dabei namentlich zu benennen. Darüber hinaus werden die Schlüsselrollen des V-Modells, wie Projektleiter, QS-Verantwortlicher und Systemarchitekt, mit Personen besetzt und deren Aufgaben und Verantwortlichkeiten entsprechend den V-Modell-Vorgaben ausgestaltet.

Die grundlegende Organisation und Durchführung der Zusammenarbeit zwischen allen Projektbeteiligten wird definiert. Dabei werden beispielsweise Besprechungen, das Vorgehen für Abstimmungsrunden, das Konfliktmanagement, die Eskalationsstrategie, die Bedingungen für die Durchführung eines formalen Entscheidungsprozesses festgelegt und dokumentiert. Zusätzlich werden Schwellenwerte definiert, deren Überschreitung zur Einleitung von Steuerungsmaßnahmen führt. Ein Beispiel dafür ist die Überschreitung von Sollwerten für die Planung um mehr als 15%. Organisationsweite Vorgaben müssen dabei berücksichtigt werden.

Für die im Rahmen des Projektmanagements zu erstellenden V-Modell-Produkte, wie Projektplan, Schätzung, Arbeitsauftragsliste und Projekttagebuch, wird festgelegt, ob und wann diese zu erstellen sind, nach welchen Methoden, Richtlinien und Standards diese Produkte auszuarbeiten sind und mit welchen Werkzeugen sie bearbeitet werden.

7. Organisation und Vorgaben zum Risikomanagement

Damit die Einschätzungen der Risiken innerhalb des Projekts nach denselben Maßstäben erfolgen, wird das im V-Modell bereits vorgesehene Risikomanagement in diesem Abschnitt ausgestaltet und konkretisiert. Dabei ist die generelle Entscheidung zu treffen, ob neben Risiken auch Chancen betrachtet werden sollen. Für Chancen wird das gleiche Verfahren wie für Risiken angewendet, deshalb wird im Folgenden nicht mehr zwischen den Begriffen Chance und Risiko unterschieden.

Hier erfolgt die Festlegung, wann und nach welchen Kriterien Risiken in einer Risikoliste dokumentiert werden. Zusätzlich muss definiert werden, mit welchen Methoden, Richtlinien und Standards und mit welchen Werkzeugen das Risikomanagement durchzuführen ist.

Dabei sind im Einzelnen die folgenden Punkte festzulegen:

- Risikoklassen zur Einstufung von Risiken
- Kriterien zur Risikoakzeptanz
- Eskalationsstufen basierend auf den definierten Risikoklassen, entsprechend den Vorgaben des Abschnitts Organisation und Vorgaben zum Projektmanagement
- Verfahren für die Dokumentation der identifizierten Risiken und der geplanten Maßnahmen
- Zeitpunkte und Vorgehen bei der Risikoidentifizierung
- Zeitpunkte für die Neubewertung von Risiken
- Zeitpunkte und Verfahren für die Planung und Durchführung von Gegenmaßnahmen

8. Organisation und Vorgaben zum Problem- und Änderungsmanagement

Problemmeldungen und Änderungsanträge werden in **Allegra** erfasst. **Allegra** ist unter https://www.trackplus.com zu erreichen.

Alle zum Problem- und Änderungsmanagement gehörenden Typen von Objekten (z.B. Problemmeldung, Änderungsantrag) und ihre Attribute (z.B. Status als "erstellt, genehmigt", "abgelehnt") sind in **Allegra** hinterlegt. Auch die Besetzung der Änderungssteuerungsgruppe (Change Control Board) für jeden Bereich sind dort über Zugehörigkeiten zu entsprechenden Gruppen hinterlegt.

9. Organisation und Vorgaben zum Konfigurationsmanagement

Im Projekt erarbeitete Produkte und für das Projekt relevante externe Produkte werden im **Allegra-Wiki** oder im Projekt-Repository in **Gitlab** abgelegt. **Allegra** ist unter https://www.trackplus.com/allegra zu erreichen, Gitlab über Allegra oder direkt unter https://www.trackplus.com/gitlab.

Lokale Arbeitsstände müssen unverzüglich, spätestens am Ende eines Arbeitstages in Allegra bzw. Gitlab gesichert werden.

9.1 Identifikation von Dokumenten in der Ablagestruktur

Die Identifikation der Dokumente erfolgt über Vorgangsnummern in Allegra bzw. einen eindeutigen Dokumentnamen in Gitlab. Auf der obersten Ebene soll die Ablagestruktur für Dokumente aus den Verzeichnisses

- PM (für Projektmanagement)
- CM (für Konfigurations- und Change management)
- QA (für Quality assurance)
- SE (für System Engineering)
- Scratch (für Hintergrundmaterial wie Präsentationen, Notizen, Zettel usw.)

bestehen.

9.2 Versionierung von Produkten

Produkte (Dokumente, Code, etc.) können versioniert werden. Produktversionen werden über "Baselines" identifiziert. Baselines haben eine Bezeichnung nach dem Muster "RELxyz", mit x, y und z als Ziffern zwischen 0 und 9.

Für Produkte, die zu einem bestimmten Datum erstellt wurden und nicht mehr fortgeschrieben werden gilt die Konvention: „ISO-Datum Produktbezeichnung“. Ein Protokoll eines Arbeitstreffens wird damit beispielsweise unter dem Namen „20190310 Protokoll Arbeitstreffen“ abgelegt.

9.3 Datensicherung und Archivierung

Produkte (Dokumente, Code, etc.) können versioniert werden. Produktversionen werden über "Baselines" identifiziert. Baselines haben eine Bezeichnung nach dem Muster "RELxyz", mit x, y und z als Ziffern zwischen 0 und 9.

Für Produkte, die zu einem bestimmten Datum erstellt wurden und nicht mehr fortgeschrieben werden gilt die Konvention: „ISO-Datum Produktbezeichnung“. Ein Protokoll eines Arbeitstreffens wird damit beispielsweise unter dem Namen „20190310 Protokoll Arbeitstreffen“ abgelegt.

10. Organisation und Vorgaben zu Messung und Analyse

Metriken sollen erlauben, Erkenntnisse für mögliche Prozessverbesserungen zu finden. Das Ziel für eine Prozessverbesserung darf sich jedoch nicht an einzelnen Metriken festmachen lassen.

Folgende Metriken werden erhoben:

- Terminliche und aufwandsmäßige Abweichung vom Plan (Earned Value Methode)
- Meilenstein-Trendanalyse
- Team Velocity (für agil arbeitende Teams)
- Problemmeldungen nach Teilkomponenten
- Anzahl wieder-eröffneter Problemmeldungen

Die Daten für diese Metriken ergeben sich ohne zusätzlichen aufwand aus den genutzten Werkzeugen.

11. Organisation und Vorgaben zum kaufmännischen Projektmanagement

In diesem Abschnitt wird das im V-Modell bereits vorgesehene Vorgehen zum kaufmännischen Projektmanagement ausgestaltet und konkretisiert. Dabei müssen die betriebs- und volkswirtschaftlichen Vorgaben der Organisation auf das Projekt abgestimmt werden. Es erfolgt die Festlegung, ob, wann und welche Produkte für das kaufmännische Projektmanagement zu verwenden sind, nach welchen Methoden, Richtlinien und Standards diese zu erstellen sind und mit welchen Werkzeugen sie zu bearbeiten sind.

Dies beinhaltet die Festlegung der Organisation sowie die Zuordnung der Rollen des kaufmännischen Projektmanagements auf Personen beziehungsweise betriebliche Organisationseinheiten. Bei der Ausgestaltung der Organisation wird in der Regel das Vier-Augen-Prinzip berücksichtigt, so dass technische und kaufmännische Aspekte ausgewogen repräsentiert sind.

Eskalationsinstanzen bei Meinungsverschiedenheiten sind meist in der betrieblichen Organisationsstruktur schon geregelt, es kann (beispielsweise bei großen internationalen Projekten) aber auch ein Lenkungsausschuss als Eskalationsinstanz festgelegt werden.

12. Organisation und Vorgaben zum Anforderungsmanagement

In diesem Abschnitt wird das im V-Modell bereits vorgesehene Vorgehen zum Anforderungsmanagement ausgestaltet und konkretisiert. Es erfolgt die Festlegung, wann und welche Produkte für das Anforderungsmanagement zu verwenden sind, nach welchen Methoden, Richtlinien und Standards diese zu erstellen sind und mit welchen Werkzeugen sie zu bearbeiten sind.

Dies beinhaltet beispielsweise die Bestimmung aller Beteiligten am Anforderungsmanagement für die gesamte Projektlaufzeit inklusive der Verantwortlichkeiten, die Definition von möglichen Zuständen wie dem Grad der Abgestimmtheit einer Anforderung, die Festlegung einer Beschreibungsschablone für Anforderungen und eventuell die Festlegung eines Werkzeugs zur Erfassung und Verwaltung von Anforderungen.

13. Organisation und Vorgaben zur Vergabe von Entwicklungsleistungen

In diesem Abschnitt ist der Vergabeprozess bis hin zur Beauftragung des Auftragnehmers zu dokumentieren. Es muss festgelegt werden, welche Produkte dabei relevant sind und nach welchen Regelungen und Vorgaben diese erstellt werden.

Neben einem Prozess zur Vorbereitung und Veröffentlichung der Ausschreibung ist festzuhalten, wie die Bewertung der eingegangenen Angebote und letztlich die Zuschlagserteilung erfolgen.

Soll die Entwicklung informationssicherheitskritischer Systeme nur an Bieter vergeben werden, die entsprechende Zertifizierungen vorweisen können, müssen hier alle relevanten Zertifikate (z.B. BSI, ISO 270xx) aufgeführt werden, die der Bieter im Rahmen des Angebots vorweisen muss.

14. Organisation und Vorgaben zu Informationssicherheit und Datenschutz

In diesem Abschnitt wird das Vorgehen in den Bereichen Informationssicherheit und Datenschutz ausgestaltet und konkretisiert. Die Ausgangslage ist eine Auflistung der für das Projekt relevanten Standards, Normen und Richtlinien sowie eine Erklärung zum geplanten Betriebsort und den Regionen, in denen das System genutzt werden darf. Aus letzteren leiten sich die rechtlichen Vorgaben her.

Hier finden sich in jedem Projekt Verweise auf organisationsweite Regelungen und Arbeitshilfen.

In Projekten eines Auftraggebers finden sich zusätzlich Aussagen darüber, wie Vorgaben an die Informationssicherheit und an den Datenschutz erstellt und an die Auftragnehmer übermittelt werden. Diese finden sich in den zugehörigen Produkten Vorgaben zur Informationssicherheit und Vorgaben zum Datenschutz.

Zudem wird festgelegt, welche sicherheitsrelevanten Produkte im Projekt zu welchem Zeitpunkt von wem erstellt werden und welche Methodik und welche Werkzeuge hier jeweils zum Einsatz kommen sollen. Der Abschnitt präzisiert in diesem Zusammenhang die Schnittstellen zu den Rollen Informationssicherheitsbeauftragter (Organisation) und Datenschutzbeauftragter (Organisation).

Für beide Bereiche ist es wichtig, die Beteiligten zu sensibilisieren und für die Fälle, in denen ihre Mitarbeit erforderlich ist (z.B. Eskalation bei einem Sicherheitsvorfall), Handlungsanweisungen zu kommunizieren. Beides wird in diesem Abschnitt konzipiert und als einzelne Maßnahmen abgebildet.

14.1 Eingesetztes Personal

Als Projektmitarbeiter darf nur eingesetzt werden, wer folgenden Anforderungen genügt:

- Die Verschwiegenheitsvereinbarung (NDA) <Dokumentname> wurde gelesen, verstanden und unterschrieben.
- Der Mitarbeiter wurde ohne Beanstandung nach <Ü1|Ü2|Ü3> sicherheitsüberprüft.
- Der Mitarbeiter hat folgende Fortbildungen absolviert oder einen vergleichbaren Wissensstand:
- <Name Fortbildung 1 zur Informationssicherheit>
- <Name Fortbildung 2 zum Datenschutz>

Der Mitarbeiter wurde gemäß <Dokumentname> auf die Einhaltung der Vorgaben zu Informationssicherheit und Datenschutz verpflichtet und der Nachweis unter <Speicherort> abgelegt.

15. Organisation und Vorgaben zum Informationssicherheits-Managementsystem

In diesem Abschnitt wird geregelt, wie die im Projekthandbuch festgelegten elektronischen Werkzeuge für die Projektarbeit in das Informationssicherheits-Managementsystem (ISMS) der Organisation eingebunden werden und welche Vorgaben aus dem ISMS für den Einsatz der Werkzeuge zu beachten sind. Beispielsweise kann festgelegt werden, dass E-Mails nur verschlüsselt an im System hinterlegte Empfänger übertragen werden dürfen.

15.1 Allgemeines

Das Projekt <Projektname> ist als sicherheitskritisch eingestuft (vgl. Kapitel Projektspezifisches V-Modell) und ist daher in das Informationssicherheits-Managementsystem (ISMS) der <Name der Organisation> eingebunden. Die Anwendung des ISMS erstreckt sich auf folgende Abläufe im Projekt: <Anwendungsbereiche>.

15.2 Ansprechpartner

	Ansprechpartner	Vertretung
ISMS Allgemein	<Kontaktdaten>	<Kontaktdaten>
Störungen, Notfälle		
Wartung		
Änderung		

15.3 Stakeholder

Folgende Personen und Gruppen sind grundsätzlich an der Sicherheit des zu entwickelnden Systems interessiert:

Stakeholder	Maßnahme zur Einbindung
Betrieb	Regelmäßige Berichterstattung
<...>	<...>

15.4 Dokumentation

Folgende Dokumente beschreiben die Rahmenbedingungen und Konzepte gemäß den Vorgaben des ISMS:

Informationssicherheitsleitlinie

im Intranet: <URL zum Dokument>

IT-Betriebshandbuch

im Intranet: <URL zum Dokument>

IT-Notfallhandbuch

im Intranet: <URL zum Dokument>

<...>

15.5 Besonderheiten des Projekts

Folgende kritische Anwendungen stellen eine Besonderheit des Projekts <Projektname> im Vergleich zu anderen Entwicklungsprojekten der <Name der Organisation> dar.

<z.B. Mongo Datenbank>

<...>

Weitere Besonderheiten betreffen die Projektorganisation sowie die zu verwendenden Kommunikationskanäle:

Einbindung Auftraggeber über gemeinsames System <z.B. JIRA>

<...>

15.6 Berichtswesen

Siehe Kapitel Berichtswesen und Kommunikationswege.

15.7 Besondere Maßnahmen

Mit der Durchführung der folgenden Maßnahmen wird auf die besondere Situation des Projekts eingegangen:

- <Maßnahme 1>
- <Maßnahme 2>

15.8 Audits

An folgenden Terminen sind Audits zur Überwachung der Sicherheitskonzeption vorgesehen:

- <TT.MM.JJJJ>
- Quartalsweise
- Halbjährlich

16. Organisation und Vorgaben zur Funktionssicherheit

In diesem Abschnitt wird das Vorgehen zur Gewährleistung der Funktionssicherheit im Projekt ausgestaltet. Dies umfasst die zu berücksichtigenden Methoden, Richtlinien und Standards sowie die einzusetzenden Werkzeuge. Zusätzlich sind Handlungsvorgaben beim Auftreten nicht akzeptabler Sicherheitsrisiken und die anzuwendenden, generellen risikomindernden Maßnahmen festzulegen.

Die generellen risikomindernden Maßnahmen werden in einer Sicherheitsstufen-Maßnahmen-Matrix definiert. In dieser Matrix werden abhängig von der Sicherheitsstufe geeignete Maßnahmen hinsichtlich der Konstruktion und Prüfung bestimmt. Bei der Festlegung der Maßnahmen kann auf existierende Sicherheitsstandards wie z.B. DIN EN IEC 61508 zurückgegriffen werden. Die darin vorgeschlagenen Maßnahmen sind projektspezifisch auszuwählen und zu konkretisieren.

17. Organisation und Vorgaben zum IT-Betrieb

Hier wird beschrieben, wie der vorgesehene Betreiber des zu entwickelnden Systems in das Projekt eingebunden wird. Insbesondere sollte die Mitarbeit des IT-Betriebs bei der Anforderungsfestlegung und der Qualitätssicherung geregelt werden.

Die Anforderungen des IT-Betriebs fließen als Vorgaben zum IT-Betrieb in das Lastenheft ein oder werden dort referenziert. Zur Überprüfung, ob die Anforderungen des IT-Betriebs korrekt und vollständig umgesetzt wurden, wird eine Prüfspezifikation Inbetriebnahme erstellt. Im Fall einer erfolgreichen Überprüfung erteilt der IT-Betrieb die Betriebliche Freigabeerklärung.

18. Organisation und Vorgaben zur Systemerstellung

In diesem Abschnitt wird das im V-Modell bereits vorgesehene Vorgehen zur Systemerstellung ausgestaltet und konkretisiert. Es erfolgt die Festlegung, wann und welche Produkte für die Systemerstellung zu verwenden sind, nach welchen Methoden, Richtlinien und Standards diese zu erstellen sind und mit welchen Werkzeugen sie zu bearbeiten sind.

Dies beinhaltet zumindest die Festlegung der anzuwendenden Entwicklungsmethoden, Entwicklungsumgebung, Technologien sowie Konfliktmanagement und Eskalationsstrategie.

Die Reports der Werkzeuge passen im Normalfall nicht zur Struktur der V-Modell XT Produkte. Die Modellierung in den Werkzeugen müssen inhaltlich die Produktmuster abdecken.

18.1 Rahmenbedingungen und Richtlinien

Das System wird unter Berücksichtigung der Anforderungen aus den relevanten Bausteinen des IT-Grundschutz-Kompendium (z.B. Softwareentwicklung, Software-Tests und -Freigaben, Entwicklung und Einsatz von Fachanwendungen) designt.

Zur Vermeidung typischer Programmierfehler und Schwachstellen sind alle Entwickler angehalten, folgende Dokumente und Standards zu beachten:

- OWASP Top Ten Project
- SEI Cert Coding Standards
- IT-Sicherheitskriterien nach <ITSEC-Vorgaben der Organisation>
- Common Criteria Protection Profile <Profil>
- The Protection of Information in Computer Systems (vgl. Eintrag SaSch75 im Literaturverzeichnis des V-Modell XT)

18.2 Getrennte Umgebungen

Für Entwicklung, Test und Produktion des Systems werden vollständig voneinander getrennte Umgebungen verwendet. Ein Zugriff auf das Produktivsystem ist dem IT-Betrieb vorbehalten. Zugriffsrechte für Entwicklungs- und Testsysteme werden vom Projektleiter vergeben.

Für die Entwicklung werden folgende Systeme verwendet:

- Datenbank: <Name>, <URL>
- Application Server: <Name>, <URL>
- <...>

Für Tests zur <Integration, Abnahme, ...> werden folgende Systeme verwendet:

- Datenbank: <Name>, <URL>
- Application Server: <Name>, <URL>
- <...>

18.3 Sichere Systementwicklung

Um zu gewährleisten, dass das System nicht bereits während der Entwicklung manipuliert wird, sind im Projekt folgende Maßnahmen vorgesehen:

Kontrollierte Änderungen im Repository (siehe Kapitel Organisation und Vorgaben zum Konfigurationsmanagement): jede Änderung wird gemäß Vier-Augen-Prinzip gesichtet, bevor sie in den Master-Strang übernommen wird.

Aufteilung der Commit-Rechte im Repository nach Kompetenzen: es wird vermieden, dass einzelne Personen auf große Bereiche des Repositories Schreibrechte haben. Stattdessen sind die Schreibrechte nach Kompetenzen gegliedert – Schreibrechte beispielsweise im QS-Bereich verhindern Schreibrechte im Entwicklungsbereich.

Identifikation und Nachvollziehbarkeit: um die unterschiedlichen Builds eines Systems eindeutig identifizieren zu können und um eine lückenlose Nachvollziehbarkeit aller Änderungen zu ermöglichen, werden alle Builds für die Test- und Produktionsumgebungen an zentraler Stelle zusammengestellt. Dazu gehört die Vergabe eindeutiger, fortlaufender Versionsnummern ebenso wie die Signierung des Ergebnisses.

Komponenten von anderen Herstellern werden stets mit genauer Versionsbezeichnung eingebunden. Insbesondere ist das selbständige, automatische Aktualisieren nicht erlaubt.

<...>

18.4 Test

Durch regelmäßige Tests wird validiert und verifiziert, dass das zu entwickelnde Systemelement den Anforderungen - funktional und nicht-funktional - genügt. Um diese Tests in den Entwicklungsprozess integrieren zu können, müssen sie bereits im Rahmen des Systementwurfs mit entworfen und durch den Entwicklungsgegenstand unterstützt werden. Dies kann beispielsweise beinhalten, dass für einzelne Funktionen des zu entwickelnden Systemelements frühzeitig Skeletons und Stubs implementiert werden, um Testabläufe zu Zeitpunkten zu unterstützen, an denen nur ein Teil der geforderten Funktionalität vorliegt. Im Rahmen der Informationssicherheit und des Datenschutzes sind folgende Tests zu entwerfen und durchzuführen:

- Funktionale Tests, um die korrekte Umsetzung von Maßnahmen der Informationssicherheit und des Datenschutzes zu verifizieren <z.B. Äquivalenzklassentest der folgenden Merkmale: <Merkmale>>
- Security-Tests, um die Einhaltung der Informationssicherheit und des Datenschutzes zu validieren:
- Reviews des Systementwurfs
- Code-Reviews durch Security-Experten
- Prüfung der Einhaltung von Vorgaben zur Code-Erstellung / Entwurfsprinzipien
- Penetrationstests des zu entwickelnden Systemelements
- Automatisierte Tests durch <Software-Werkzeuge>
- <...>

Beim Entwurf der Tests darf der Fokus nicht nur auf den Positiv-Fällen (gewünschte Abläufe für legitime Nutzer des Systemelements) liegen, sondern insbesondere auf den Negativ-Fällen (Verhinderung nicht legitimer Nutzung des Systemelements).

19. Vorgaben für das Projekthandbuch der Auftragnehmer

In diesem Abschnitt kann der Auftraggeber die unterschiedlichsten Vorgaben für die Planung und Durchführung des Projektes beim Auftragnehmer festlegen. Sie werden hier dokumentiert und dann im Abschnitt Leistungsbeschreibung aller Ausschreibungen übernommen und gegebenenfalls angepasst. Die Vorgaben können beispielsweise den zu verwendenden Entwicklungsprozess, das Tailoring, die zu verwendende Infrastruktur und das Vorgehen bzgl. der Sicherheit umfassen.

19.1 Allgemeines

Der Auftragnehmer regelt in seinem Projekthandbuch die nachfolgenden Aspekte und gewährt dem Auftraggeber auf Anforderung Einblick in sein Projekthandbuch.

19.2 V-Modell XT mit Tailoring

Der Auftragnehmer setzt den Standard V-Modell XT 2.x oder eine dazu konforme organisationsspezifische Anpassung ein.

Das System wurde als sicherheitskritisch eingestuft. Im Rahmen des Tailorings nutzt der Auftragnehmer die angebotenen Vorgehensbausteine zur Informationssicherheit und zum Datenschutz.

19.3 SSDLC

Um eine Ausrichtung des Projekts auf die Zielsetzung der Informationssicherheit und des Datenschutzes zu gewährleisten, basiert die Entwicklungsmethodik des Auftragnehmers auf einem etablierten Methodenbaukasten für die Entwicklung sicherer Software-Systeme (englisch: SSDLC). Im Projekthandbuch werden die Methoden benannt und für den Bereich der Systementwicklung detailliert.

19.4 Bereitstellung eines ISMS

Der Auftragnehmer muss ein Informationssicherheits-Managementsystem (ISMS) einführen und etablieren und alle von ihm für das Projekt benötigten Werkzeuge in das ISMS einbinden. Er muss dies dem Auftraggeber nach Aufforderung offenlegen und von diesem geforderte Änderungen oder Ergänzungen zur Erfüllung projektspezifischer Vorgaben zum ISMS umsetzen.

19.5 Dokumentation

Alle Sicherheitsvorfälle, die das Projekt betreffen, werden zeitnah an den Projektleiter des Auftraggebers kommuniziert und zudem vollständig dokumentiert.

19.6 Problem- und Änderungsmanagement

Für das Anforderungsmanagement sowie für das Problem- und Änderungsmanagement betreibt der Auftragnehmer ein Allegra-System. In Abstimmung mit dem Auftraggeber richtet er die notwendigen Zugriffsrechte ein und beschreibt die im Projekt genutzten Dialoge, Felder, Zustände und Abläufe.

19.7 Konfigurationsmanagement

Der Auftragnehmer betreibt ein Versionsverwaltungswerkzeug und gewährleistet, dass der Entwicklungsstand dort tagesaktuell hinterlegt ist. Er gewährleistet zudem, dass nur Berechtigte Zugriff auf das Versionsverwaltungswerkzeug im jeweils benötigten Umfang haben.

19.8 Build-Prozess

Der Auftragnehmer gewährleistet folgende Eigenschaften des Build-Prozesses für Software-Artefakte:

Alle für einen Build benötigte Artefakte (Source Code, Skripte, Konfigurations-dateien, etc.) werden aus dem Versionsverwaltungswerkzeug bezogen.

Jedem Artefakt ist eine übergreifend eindeutige Versionsnummer zugeordnet. Versionsnummern werden fortlaufend hochgezählt.

Anhand der Versionsnummer ist dokumentiert, welche Bestandteile für den jeweiligen Build herangezogen wurden (z.B. Versionsnummer und Signatur externer Einheiten).

Es ist gewährleistet, dass jeder Build mit binär identischem Ergebnis reproduziert werden kann.

Alle auszuliefernden Artefakte werden vom Auftragnehmer elektronisch signiert.

19.9 Kommunikation

Die Kommunikation zwischen Auftraggeber und Auftragnehmer erfolgt auch elektronisch. Folgende Kommunikationswege bzw. Plattformen sind dabei vom Auftraggeber vorgegeben und müssen vom Auftragnehmer geeignet berücksichtigt werden:

- Mit <PGP|S/MIME> verschlüsselte E-Mails
- Dokumentenablage auf dem zentralen <BSCW|Sharepoint|TFS>-Server

Der Auftragnehmer kann weitere Kommunikationswerkzeuge vorschlagen. Er stimmt sich dazu mit dem Auftraggeber ab und stellt die für die Nutzung erforderlichen Maßnahmen auf Seiten des Auftraggebers detailliert dar.

19.10 Sicherheitskonzeption

Der Auftragnehmer gewährleistet, dass die von ihm zu erstellende Sicherheitskonzeption in einem Format vorgehalten wird, das vom Werkzeug <verinice> ohne inhaltliche Verluste importiert werden kann. Er stimmt sich dazu nach Auftragserteilung mit dem Auftraggeber ab.

19.11 Sicherheitsüberprüfung

Aufgrund der folgenden Gegebenheiten wird für alle Mitarbeiter des Auftragnehmers im Projekt die Sicherheitsstufe <Ü1|Ü2|Ü3> gefordert:

- Zugang zu Verschlusssachen im Rahmen der Tätigkeiten im Projekt.
- Zugang zu personenbezogenen oder vertraulichen Daten im Projekt.

Der Auftragnehmer verpflichtet sich, nur solche Mitarbeiter einzusetzen, die eine geeignete, aktuelle, erfolgreiche Sicherheitsüberprüfung nachweisen können. Die Verpflichtung erstreckt sich auch auf alle im Projekt eingesetzten Mitarbeiter der Unterauftragnehmer.

19.12 Eignung bzgl. Informationssicherheit und Datenschutz

Der Auftragnehmer verpflichtet sich, nur solche Mitarbeiter einzusetzen, die

- auf die Einhaltung der Vorgaben zur Informationssicherheit und der Vorgaben zum Datenschutz nachweislich verpflichtet wurden.
- über die notwendigen Kenntnisse zu Informationssicherheit und Datenschutz verfügen; er sorgt ggf. unaufgefordert für notwendige Fortbildungsmaßnahmen.
- in <Deutschland|der Europäischen Union|der Schweiz> ihren ständigen Wohnsitz haben.

Die Verpflichtung erstreckt sich auch auf alle im Projekt eingesetzten Mitarbeiter der Unterauftragnehmer.

Der Auftragnehmer weist darüber hinaus Kenntnisse und Erfahrung der für den Einsatz als Datenschutz- oder Informationssicherheitsverantwortlicher vorgesehenen Mitarbeiter nach, beispielsweise durch

- mindestens <zwei> Referenzprojekte vergleichbarer Größe und Art in den vergangenen <fünf> Jahren.
- Zertifikate/Teilnahmebescheinigungen einschlägiger Ausbildungszentren.

Der Auftragnehmer verpflichtet sich, nur Unterauftragnehmer einzusetzen, die

- in <Deutschland|der Europäischen Union|der Schweiz> ansässig sind.
- wirtschaftlich und rechtlich unabhängig von Dritten und von Staaten außerhalb des genannten Gebiets sind.

20. Berichtswesen und Kommunikationswege

In den vorhergehenden Themen wurden die Organisation und Vorgaben für die unterschiedlichen Aufgaben der Planung und Durchführung von Projekten festgelegt. In diesem Abschnitt wird ein Überblick über das dabei festgelegte Berichtswesen und die Kommunikationswege dargestellt. Dies beinhaltet beispielsweise die getroffenen Festlegungen, wer wann welche Informationen in welcher Form an wen zu liefern hat.

20.1 Verhaltensregeln

Für alle Beteiligten gelten hinsichtlich der Kommunikation über Projektinhalte folgende Verhaltensregeln:

- Keine Kommunikation über vertrauliche Inhalte im öffentlichen Raum (z.B. Telefonieren im Zugabteil, Diskussionen im Restaurant)
- Kein Arbeiten an vertraulichen Dokumenten (inkl. E-Mail) im öffentlichen Raum (z.B. im Wartebereich des Flughafens)
- Keine Präsentationen in Räumen, die von außerhalb eingesehen werden können (etwa von Häusern auf der anderen Straßenseite)
- Kein Arbeiten von zuhause aus

Sensible Dokumente und Inhalte verlassen nie den geschützten Bereich. Insbesondere werden vertrauliche Dokumente nicht ausgedruckt und mitgenommen.

20.2 Sichere Kommunikation innerhalb der Organisation

Folgende Kommunikationswege sind im Rahmen des ISMS für die Projektarbeit zugelassen (siehe <Verweis auf ISMS bzw. Anwendungshilfen>):

- Verschlüsselte und signierte E-Mail mit S/MIME oder PGP
- Dokumentenmanagement über den Server <Servername>
- Treffen in den abgesicherten Besprechungsräumen <Raumnummern>

Dabei sind die jeweils festgelegten Maßnahmen zu beachten.

20.3 Sichere Kommunikation mit anderen Organisationen

Gemäß den geschlossenen Verträgen sind folgende Kommunikationswege für die Zusammenarbeit vorgesehen:

- Verschlüsselte und signierte E-Mail mit S/MIME oder PGP
- Dokumentenmanagement über den Server <Servername>
- Treffen in den abgesicherten Besprechungsräumen <Raumnummern>

20.4 Notfall-Management

Im Fall von Sicherheitsvorfällen, in denen insbesondere vertrauliche Information an Dritte gelangt sein können, ist <Ansprechpartner> zu benachrichtigen