Thüringer Polizei Landeskriminalamt

Technische und organisatorische Rahmenbedingungen zur Einführung und zum Betrieb von IuK-Lösungen im Informationssystem der Thüringer Polizei (ISTPOL)

Geheimhaltungsgrad:	
Kurzbezeichnung:	**Rahmenbedingungen zur Einführung und zum Betrieb von IuK-Lösungen im ISTPOL**
QM-Nummer:	**QM-000-LL-1027-2.4-F**
Geltungsbereich:	**ThPol**
Aktenzeichen/VIS-Nr:	**710-2946-102/2019-121426/2023**
zuständige Organisationseinheit:	**Abteilung 7/Dezernat 71**
Bestätigt am:	**19.12.2023**
Inkrafttreten:	**19.12.2023**
Prüfdatum:	**19.12.2026**
Dokumentenstatus:	**F = freigegeben**

Impressum

Landeskriminalamt Thüringen
Kranichfelder Straße 1
99097 Erfurt

Telefon	+49 (0)361 57 43 - 109
Fax	+49 (0)361 341 - 1450
E-Mail	lka@polizei.thueringen.de
Internet	https://polizei.thueringen.de/landeskriminalamt

Inhaltsverzeichnis

1 Zweck, Ziele

Das Dokument beschreibt in Form einer Richtlinie die technisch-organisatorischen Rahmenbedingungen des Informationssystems der Thüringer Polizei (ISTPOL).

Potentielle Dienstleister/Lieferanten sollen einen, aus polizeilicher Sicht, verfahrensunabhängigen Überblick über dieses Informationssystem bekommen und die Rahmenbedingungen für die Integration neuer Hard- oder Software bzw. Systeme oder Verfahren kennen.

Die polizeilichen Kommunikationssysteme, wie z. B. das TK-Netz für Sprache, sind eng mit dem klassischen IT-Netz des ISTPOL verbunden, z. T. integriert. Für Netzübergänge und gemeinsam genutzte Dienste der Kommunikationslösungen gelten diese Regelungen analog.

Nicht berücksichtigt, somit ausgeschlossen von dieser Richtlinie, sind spezifische IT-Systeme, geräteinterne Software und Einzelsysteme, welche keine direkte Schnittstelle in das IT-Netz bzw. zu Systemen im ISTPOL besitzen und keine polizeilichen Daten verarbeiten (z.B. Messgeräte, spezielle Kommunikations- und Überwachungsanlagen).

Es werden im Dokument die Rahmenbedingungen sowie Vorgaben der Zentralstelle für polizeiliches IuK Wesen (ZpIuK) zu grundsätzlichen Themen grob dargestellt. Für Rückfragen oder Detailinformationen ist die ZpIuK im Rahmen der Angebotserstellung bzw. Realisierung zu kontaktieren.

Sofern in dem spezifischen Leistungsverzeichnis/Lastenheft nichts Anderes geregelt ist, sind die im Dokument aufgeführten Anforderungen durch den Bieter bei der Angebots-/ Konzepterstellung sowie durch den Auftragnehmer/Lieferanten bei der Vertrags-ausführung/Realisierung verbindlich zu berücksichtigen. Technologische oder fachliche Abweichungen von diesen Anforderungen sind im Vorfeld aufzuzeigen und zwingend abzustimmen. Ausnahmen bedürfen einer expliziten schriftlichen Bestätigung durch die ZpIuK, in Ausschreibungsverfahren sind dahingehende Bieterfragen zu stellen.

Die Begriffe wie Verfahren und Anwendung, die Begriffe wie Vorhaben und Projekt und die Begriffe wie Dienstleister, Auftragnehmer, Lieferant, Realisierungspartner werden im Dokument gleichlautend verwendet.

2 Allgemeine Information

Entsprechend des Thüringer Polizeiorganisationsgesetzes (POG) ist das Landeskriminalamt Thüringen (TLKA) Zentralstelle für das polizeiliche Informations- und Kommunikationswesen.

Der ZpIuK obliegt damit die Zuständigkeit für die Planung, den Betrieb und die Weiterentwicklung des ISTPOL in seiner Gesamtheit und der damit verbundenen organisatorischen Arbeiten.

Durch die ZpIuK wird mit Unterstützung der für den IT-Betrieb zuständigen Organisationseinheiten der Behörden, Bildungseinrichtungen und des Thüringer Landesrechenzentrums (TLRZ) eine hohe Verfügbarkeit des ISTPOL gewährleistet. Dabei wird entsprechend der polizeifachlichen Anforderungen durch die ZpIuK ein 24-Stunden-Betrieb an sieben Tagen pro Woche sichergestellt.

Die ZpIuK ist verantwortlich für die Betreuung der Schnittstellen polizeilicher Verfahren untereinander und zu außerpolizeilichen Diensten und Fremdverfahren.

3 Beschreibung des IT-Systemverbundes ISTPOL

3.1 Allgemein

Das Informationssystem der Thüringer Polizei besteht im Wesentlichen aus zentralen Komponenten (Speichersysteme, Server, netzverteilende Systeme und weiteren Komponenten im Rechenzentrum (RZ)) sowie dezentraler Infrastruktur und Technik für ca. 5900 Arbeitsplätze im geschlossenen Netz der Thüringer Polizei. Dazu gehören LAN/WAN- und TK-Systeme, Standardprodukte, Lizenzen, Arbeitsplatzkonfigurationen und Drucker.

Durch die ZpIuK werden ca. 60 zentrale, hochverfügbare Fachverfahren und ca. 130 Verfahren und Standardprodukte sowie die dazu notwendigen IT- Basisdienste (Services) betrieben und bei entsprechenden rechtlichen, fachlichen, technischen oder informationssicherheitsrelevanten Erfordernissen weiterentwickelt.

3.2 Zentral (Rechenzentrum)

Die zentralen Komponenten bestehen in der Regel aus x86-basierten Systemen der Firma HP Enterprise und nutzen als Betriebssysteme Linux (RHEL® / SLES® / OracleLinux / Debian), MS WINDOWS® und herstellerspezifische Hypervisor (ESXi). Diese werden auf Basis einer Vereinbarung zur Auftragsdatenverarbeitung (Outsourcing-Vertrag zu Basisdiensten) im Thüringer Landesrechenzentrum (TLRZ) bzw. durch die ZpIuK selbst betrieben. Die Serverräume befinden sich dabei an Technikstandorten wie dem TLKA, der Landespolizeidirektion (LPD, Außenstandort LEZ) und dem TLRZ, welche einen Aufbau von redundanten Hochverfügbarkeitslösungen zulassen.

Die Infrastrukturkomponenten der Technikzentren (USV/Klimatisierung/Gebäudehülle) besitzen eine theoretische Verfügbarkeit von 99,9 %.

Als Datenbanksysteme kommen derzeit in der Regel ORACLE® und MS SQL® zum Einsatz.

Hochverfügbare Anwendungen werden in Clustern betrieben.

Aufgrund der strategischen Ausrichtung der ZpIuK werden zentrale Systeme zunehmend in virtualisierten Umgebungen abgebildet, wobei Blade-System basierte Technik im Verbund mit Hypervisorn genutzt werden (z.B. VMWare, Proxmox…).

Um den Anforderungen der ortsunabhängigen Arbeit zur Wahrung von Flexibilität und Einsatzbereitschaft gerecht zu werden, kommen gleichfalls eine Terminalserver-Lösung von Citrix® als auch eine VPN-basierte Anbindung von eigenen mobilen Endgeräten zum Einsatz.

Die Thüringer Polizei nutzt unter anderem folgende Lizenzen:

- die landesweite Lizenz für Standard Oracle Datenbanken (nutzerbasierendes Lizenzmodell)
- für jeden Arbeitsplatz im ISTPOL Microsoft Office 2016® sowie MS WINDOWS 10 Enterprise
- landesweite Lizenzen für das Dokumentenmanagementsystem VISkompakt® der Fa. PDV-Systeme GmbH, das ITIL-Servicemangement Werkzeug Omnitracker, für den CITRIX® Terminal Server, GDI-Infrastruktur (ESRI) und GIS-Karten
- Lizenzen für das Enterprise Content Management System (OS/ECM®) der Fa. Optimal Systems
- Einzelplatzlizenzen von Analyst Notebook®, MS Visio®, MS Project ®, Acrobat Pro®

Das genaue Lizenzmodell des jeweiligen Standardproduktes ist bei Bedarf in der ZpIuK zu hinterfragen. Sofern keine ausdrückliche Aufforderung im Leistungsverzeichnis erfolgt, werden Microsoft-Lizenzen über den Rahmenvertrag des Bundes beschafft und als Beistellleistung zur Verfügung gestellt.

Ein zukünftiger Lösungsanbieter soll vorrangig vorhandene Lizenzen und deren Synergieeffekte nutzen, aber ebenfalls auf Open Source basierte Lösungen setzen.

3.3 Dezentral (in den B/B der Thüringer Polizei)

Im dezentralen Bereich der Behörden und Bildungseinrichtungen werden Infrastrukturserver (Datei- und Druckdienste, Softwareverteilung, Antivirus, Active Directory) betrieben.

Weiter werden etwa 5900 vernetzte PC und Notebooks unter dem Betriebssystem Windows 10 Enterprise (bzw. WINDOWS 8.1 Professional® in Ausnahmefällen) als Endgeräte betrieben. Als Standardbrowser kommt der MS Edge zum Einsatz. Neue Produkte sind kompatibel zu Win 10 Enterprise (min. 20H2) und MS Edge auszuführen.

Client-Software ist für eine automatisierte, unbeaufsichtigte Installation zu paketieren und wird über das Produkt Microsoft Endpoint Configuration Manager (MECM)® zentral ausgerollt.

An Drucktechnik (ca. 1000 Geräte) werden überwiegend Geräte der Fa. KYOCERA® unterschiedlicher Baureihen genutzt.

Als Standardanwendungen und zur Bürokommunikation sind folgende Produkte im Einsatz:

- Microsoft Office Suite 2016® (Word, Excel, PowerPoint)
- VLC Mediaplayer (zum Abspielen von Audio und Videodateien)
- Acrobat® PDF Reader
- Irfanview® (zur Anzeige von Bilddateiformaten)
- Aktuelle Version der Java® Run Time Environment
- MS Edge
- Notepad++®
- PDF-Creator® (zum Erzeugen von PDF Druckausgaben)
- .Net Framework
- MS-Visio® Viewer
- Virenscanner MS Defender
- Microsoft Outlook® mit MS Exchange® 2016 / 2019

Die Thüringer Polizei autorisiert und verwaltet die Nutzer und PC-Technik im Active Directory (Single Domäne).

3.4 Netz

Die WAN Kommunikation der Hard- und Softwarekomponenten erfolgt verschlüsselt in einem in sich abgeschlossenen logischen Netz (VPN auf Basis IPSec), basierend auf der Infrastruktur des Corporate Network Freistaat Thüringen (CN FT).

Die zur Verschlüsselung eingesetzten Systeme sind durch das BSI für die Übertragung von Daten bis Verschlusssache „Nur für den Dienstgebrauch“ (VS-NfD) zugelassen. Die

Aufbereitung der Daten aus dem LAN für die IPSec Verschlüsselung erfolgt mittels Generic Routing Encapsulation (GRE) Protokoll und einer Maximum Transfer Unit (MTU) 1380.

Die eingesetzten Layer-3 Switche senden bei Paketen, die die eingestellte MTU Size am GRE Tunnel überschreiten, an den Absender eine ICMP Fehlermeldung Typ 3 Code 4 „Fragmentation Needed“ zurück. Die Daten werden fragmentiert und versendet. Eine feste Einstellung einer MTU Size kleiner als die WAN MTU Size 1380 kann für Clients oder Server notwendig sein.

Die aktiven Netzkomponenten werden zentral administriert.

Es werden das Protokoll SNMP verwendende Netzwerkmanagementsysteme eingesetzt.

Die Anbindung der Dienststellen und Behördeneinrichtungen erfolgt mit einer Bandbreite zwischen 2 und 1000 Mbit/s über das CN FT.

Die drei Technikstandorte TLKA, LPD, TLRZ und große Dienststellen sind redundant an das CN FT angebunden.

Zusätzlich sind die drei Technikstandorte TLKA, LPD, TLRZ untereinander mit Datendirektverbindungen verbunden (zw. Standort LPD und Standort TLRZ 2x10 Gbps sowie zw. Standort TLKA und Standort LPD bzw. TLRZ je 1 Gbps WAN Bandbreite).

In den lokalen Netzen der Technikstandorte TLKA, LPD, TLRZ und BZ sind Kapazitäten im 10 GBit Bereich vorhanden.

Alle Netzübergänge werden über ein Firewallsystem abgesichert.

Kommunikationsverbindungen unter Umgehung des Firewallsystems werden nicht realisiert.

Ein direkter Zugriff auf Systeme und Plattformen im Internet und nicht vertrauenswürdige Netze ist nicht zugelassen.

Wählbare Netzübergänge, auch temporärer Art, sind nicht zugelassen. Fernwartungszugriffe externer Dienstleister sind für sicherheitsüberprüftes Personal u. U. möglich.

Für die Nutzung des Internets stehen Einzelplatzsysteme mit eigenem Anschluss an das Internet zur Verfügung.

Mobile Endgeräte (Laptops) werden über einen standardisierten Zugang über VPN in das ISTPOL eingebunden.

Für die Netzanbindung über das CN FT wird von folgenden Verfügbarkeiten der Standorte ausgegangen:

Standort TLKA:	99,9 % im Monatsmittel
Standort LPD:	99,9 % im Monatsmittel
LPI / KPI Standorte:	99,5 % im Monatsmittel
PI Standorte:	99,0 % im Jahresmittel
Standort TLRZ:	99,9 % im Monatsmittel

3.5 Kataloge

Die Datenerfassung erfolgt grundsätzlich maskengesteuert. Dabei soll u. a. aus Gründen der Qualitätssicherung und Standardisierung die kataloggestützte Erfassung realisiert werden.

Im Rahmen einer IT-Kooperation mit anderen Bundesländern wird ein gemeinsames zentrales „Stammdatenverwaltungssystem (SDV)“ betrieben. Bei neu einzuführenden Verfahren ist generell die Nutzung vorhandener Kataloge vorgeschrieben. Heute stehen ca. 400 Kataloge im zentralen SDV zur Verfügung.

Zur Entkopplung der Verfahren und aus Gründen der Geschwindigkeit wird empfohlen, die durch das Verfahren genutzten Kataloge in die Datenbank des Verfahrens zu spiegeln und über Batch–Schnittstelle dieses Abbild der Katalogwerte regelmäßig zu aktualisieren.

Spezifische Katalogwerte für Verfahren können entweder durch Erweiterung der zentralen Katalogverwaltung oder in begründeten Ausnahmefällen im Verfahren selbst gepflegt werden (Ausnahmegenehmigung der ZpIuK ist im Vorfeld einzuholen).

Zur Sicherstellung der Datenqualität muss grundsätzlich eine Freigabeprozedur (meist zentral) von Katalogwerten realisiert werden (Vieraugenprinzip).

Die Kataloge müssen sich am XPolizei-Standard orientieren. Dazu stehen die entsprechenden XML-Schemata zur Verfügung.

3.6 Zugriffssteuerung und Berechtigungen

Über eine Berechtigungsverwaltung sind zuständigkeitsbezogene Zugriffe (Bearbeitung und Recherche) auf die jeweiligen Daten zu realisieren. Zur Abbildung der Geschäftsprozesse ist es notwendig, die Berechtigungen auf jede Einzelfunktion zuweisen zu können.

Der Zugriff kann auf einzelne Objekte, unterschiedliche Bereiche bis hin zu einzelnen Datenfeldern (mit unterschiedlichen Funktionen wie z. B. Lesen, Erfassen, Ändern, Bearbeiten, Einfügen, Löschen, Erweitern von Programmkomponenten) erfolgen. Neben vorgegebenen Standard-Rollen müssen auch änderbare Rollen entsprechender Benutzer in beliebigen Kombinationen durch die „Zentrale Berechtigungsverwaltung“ der ZpIuK definiert werden können. Zugehörigkeiten zu verfahrensspezifischen Berechtigungsprofilen und Berechtigungsrollen sind im Active Directory (AD) in Gruppenobjekten abzubilden.

Die Zugriffssteuerung und Berechtigung basiert für das jeweilige Verfahren auf einem durch den Bedarfsträger zu erstellenden Rechte- und Rollenkonzept.

3.7 Authentifizierung/Autorisierung

Die ZpIuK hat die zentrale Nutzerverwaltung über das zentrale Verzeichnis im Active Directory der Thüringer Polizei implementiert.

Neue Verfahren müssen Single-Sign-On (SSO) Funktionen mit Authentifizierung durch das AD unterstützen. Dieses Verfahren ist vom Softwarelieferanten zu implementieren.

3.8 Schnittstellen

3.8.1 Stammdatenverwaltungssystem SDV

Durch neue Verfahren sind grundsätzlich bestehende Kataloge im SDV zu nutzen bzw. wenn zwingend notwendig, Neuaufnahmen zu unterstützen. Zur Gewährleistung zyklischer Katalog-Updates ist eine entsprechende Schnittstelle zum zentralen Katalogserver (ZKS) vorzusehen. Dieser wird im Jahr 2023 beginnend schrittweise durch den "Basisdienst Kataloge" im Programm Polizei 20/20 abgelöst.

Dem SDV liegt eine PostgreSQL-Datenbank zugrunde, der ZKS arbeitet mit ORACLE®-basierten Datenbanken. Der Betrieb der SDV wird von der Landeszentrale für polizeiliche Dienste (LZpD) in Nordrhein-Westfalen sichergestellt.

3.8.2 Berechtigungsverwaltung und Nutzerdaten - Active Directory

Im AD sind nutzerspezifische Daten wie Name, Vorname, E-Mail-Adresse, Organisationseinheit und Diensttelefon gespeichert.

Standardisierte Schnittstellen auf LDAP/Kerberos/ADFS-Technologie sind zu nutzen. Dieses Verzeichnis ist das führende System für Mitarbeiterdaten der Thüringer Polizei. Andere Datenbanken mit Nutzerdaten müssen sich anhand dieser Daten ausrichten.

Eine Schnittstelle zum Personalverwaltungssystem der Thüringer Polizei ist nicht zulässig.

3.8.3 Standardisierte Im- und Exportschnittstelle

Für die Sicherstellung der Kommunikation mit anderen Systemen ist grundsätzlich eine standardisierte Im- und Exportschnittstelle auf XML-Basis/Webservice vorzusehen.

Für Schnittstellen zwischen Verfahren sind detaillierte Dokumentationen und Fehlerroutinen gefordert. Die Dokumentation der Schnittstelle in Form einer „Schnittstellenvereinbarung“ muss die Funktion der Schnittstelle, Dateninhalte, Prozessabläufe, Zeitpläne und Beschreibung der Fehlerroutinen enthalten. (Template und Inhaltsverzeichnis wird zur Verfügung gestellt.) Beim Aufbau neuer Schnittstellen ist die Kompatibilität zum XPolizei-Standard sicherzustellen.

3.9 IT-Basisdienste

Im MS WINDOWS-Umfeld kommen **ADS** und **DHCP** zum Einsatz.

Die Softwareverteilung im MS WINDOWS-Umfeld erfolgt mit dem Produkt MS Endpoint Configuration Manager®.

Ein **Antivirussystem** (z. Zt. MS Defender) ist implementiert und zwingend auch auf Serversystemen einzusetzen.

Es sind dezentrale **Datei-/Druckserver** (MS) und **Backupsysteme** (HP-Dataprotector) im Einsatz.

Die Namensauflösung erfolgt durch **DNS** als Bestandteil des AD Verbundes.

Für die Einwahl mobiler Endgeräte (siehe 3.4) und die Authentifizierung für ausgewählte Verfahren wird derzeit die **PKI** der DOI genutzt. Neu eingeführte Produkte müssen die Verwendung mit einer organisationseigenen PKI ermöglichen.

Die Zeitsynchronisation aller Systeme wird zentral über **NTP** geregelt.

Als **Mail**system wird flächendeckend MS-Exchange 2016® (zukünftig MS Exchange 2019®)

eingesetzt.

Das **Monitoring** erfolgt generell mittels ICINGA®/NagVis® als auch WhatsUp Gold. Der Lieferant hat die notwendigen MIB's und Schwellwerte für die Hardware-, Ressourcen- und Anwendungsüberwachung zur Verfügung zu stellen und die graphische Darstellung in NagVis® zu konfigurieren. Für Infrastrukturserver kann auch WhatsUp Gold® zum Einsatz kommen.

Als **User Help Desk-**, **Trouble Ticket System, Wissensmanagement** und **CMDB** kommt das Tool Omnitracker der Fa. Omninet zum Einsatz. Neue Technik muss zwingend in der CMDB erfasst werden. Durch den Lieferanten neuer Systeme sind entsprechende Importfiles bereitzustellen.

Zur Umsetzung des Intranets der Thüringer Polizei sind mehrere Web-Server im Einsatz, ein **CMS** für das Intranet ist im ISTPOL basierend auf TYPO3 implementiert.

4 Grundsätzliche Anforderungen

4.1 Gesetze, Richtlinien und Standards

Außer den Interessen der ZpIuK sind bei der Realisierung alle einschlägigen gesetzlichen und behördlichen Bestimmungen verbindlich einzuhalten.

Die ZpIuK verweist insbesondere auf die nachstehenden Gesetze, Richtlinien und Standards in der jeweils gültigen Fassung, die grundsätzlich zu berücksichtigen sind:

- Polizeiaufgabengesetz des Freistaates Thüringen (ThürPAG)
- Thüringer Datenschutzgesetz (ThürDSG)
- Thüringer Verordnung über Aussonderungsprüffristen bei polizeilicher Datenspeicherung (ThürPolAPrüffristVO)
- Einschlägige ISO-/EN-/DIN-Normen
- BSI Standards 200-1 bis 200-4, das IT-Grundschutz-Kompendium sowie für das Verfahren zutreffende technische Richtlinien des BSI
- Leitlinie für Informationssicherheit der Thüringer Polizei
- Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behinderungsgleichstellungsgesetz
- Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten (Bildschirmarbeitsverordnung)
- XPolizei-Standard

Die genannten Gesetze und Normen liegen bei der ZpIuK zur Einsichtnahme bereit.

4.2 Rangfolge von allgemeinen Richtlinien, Vorgaben und projektspezifischen Anforderungen

In den Unterlagen werden oft Anforderungen aus unterschiedlichen Rechtsquellen vorgegeben.

Wurde im Einzelfall in den Unterlagen keine detaillierte Regelung getroffen, so gilt folgender Grundsatz: spezifische Anforderungen können allgemeine Vorgaben einschränken oder präzisieren. Sie gelten in folgender Reihenfolge:

- Anforderungen des Pflichtenheftes/Leistungsverzeichnis (inklusive der Anlagen) vor
- Vorgaben, Standards und Richtlinien der ZpIuK vor
- Vorgaben des Thüringer Innenministeriums vor
- Vorgaben des Freistaates Thüringen vor
- allgemeinen Richtlinien

4.3 Nutzungsrechte

Für Verfahren und Projekte gilt grundsätzlich für alle Auftragnehmer und Realisierungspartner:

- Auslieferungen in elektronischer Form werden nutzungs- und urheberrechtlich der Lieferung in Papierform gleichgestellt.
- Sämtliche durch den Auftragnehmer/Lieferanten im Rahmen der Leistungserbringung erstellten Unterlagen, Konzepte und Dokumentationen gehen in das Eigentum der ZpIuK über und können durch die ZpIuK zur internen Verwendung verändert und fortentwickelt werden, sofern sie nicht durch allgemeine Rechte Dritter geschützt sind.
- Das Nutzungsrecht gilt auch für gleich- oder nachgelagerte Behörden und Einrichtungen sowie für externe Dienstleister, welche das TLKA mit der Erbringung von Serviceleistungen beauftragt.
- Für entwickelte Anwendungen und Software mit nicht ausschließlichen Eigentums- oder Nutzungsrechten ist ein Escrow Agreement zur Hinterlegung der Software und Quellcodedokumentationen bei einem dt. Notar zur Herausgabe an die ZpIuK im Fall des Ausfalles des Auftragnehmers/Lieferanten oder bei schweren qualitativen Leistungsstörungen, welcher der Auftragnehmer/Lieferant nicht in einem angemessenen Zeitraum behebt, zwingend abzuschließen. Ebenfalls ist eine versiegelte Übergabe zur Hinterlegung in der ZpIuK möglich.

5 Anforderungen an Projektmethodik und Umsetzung

Die wesentlichen Anforderungen an Projektmanagementmethoden, -prozesse und -werkzeuge richten sich grds. nach den Vorgaben des Dezernat 73 - Multiprojektmanagement des TLKA. Eine zentrale Grundlage für Projekte bildet hierbei das Multiprojektmanagement Handbuch (QM-000-HB-0969).

Zur Gewährleistung der Einhaltung der verbindlichen Vorgaben bei IuK-Projekten oder projektähnlichen Realisierungen etabliert und vermittelt das Dezernat 73 die Projektstandards und -methoden und stellt entsprechende Unterstützungsleistungen für Projekte als Competence Center Projektmanagement bereit.

6 Anforderungen an die Zielsysteme (neue Hard- und Software)

Nachfolgend werden das Zielsystem und die technologischen Vorgaben und Rahmenbedingungen beschrieben.

6.1 Grundanforderungen

6.1.1 Anforderungen an die Ergonomie

Die Bedienoberflächen (GUI/NUI) sind nach ergonomischen Gesichtspunkten zu gestalten. Die einzelnen Ansichten müssen frei auf einem Mehr-Bildschirm-Arbeitsplatz positionierbar und individuell durch jeden Anwender bzw. jede Anwendergruppe zuordenbar sein. Funktionsabläufe müssen sich aus dem Hauptmenü, wichtige Funktionen durch zugeordnete Symbole (Icons) bzw. durch Funktionstasten starten lassen. Wichtige situationsabhängige Funktionen müssen durch eigene Schaltflächen im Programmfenster oder durch Kontextmenüs realisiert werden. Bei gleichartigen Arbeitsgängen in unterschiedlichen Programmteilen sollen gleiche Verfahrensweisen zur Anwendung kommen.

Gefordert wird eine ruhige, intuitiv bedienbare Oberfläche entsprechend den Grundsätzen moderner Gestaltung von HMI (human-machine-interface nach ISO 9241).

Als Grundlage für GUI / NUI gelten im Besonderen folgende Normen:

- DIN EN ISO 9241-12:2000 (Informationsdarstellung)
- DIN EN ISO 9241-13:2000 (Benutzerführung)
- DIN EN ISO 9241-14:2000 (Dialogführung mittels Menüs)
- DIN EN ISO 9241-15:1999 (Dialogführung mittels Kommandosprachen)
- DIN EN ISO 9241-129:2010 (Leitlinien für die Individualisierung von Software)
- DIN EN ISO 9241-20:2008 (Leitlinien für die Zugänglichkeit der Geräte und Dienste in der Informations- und Kommunikationstechnologie (IKT))
- DIN ENV 26385 “Prinzipien der Ergonomie in der Auslegung von Arbeitsplatzsystemen”
- DIN EN 29241-3-/ ISO 9241-3- “Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten, Anforderungen an visuelle Anzeigen”

- DIN EN ISO 9241 “Ergonomische Anforderungen für Tätigkeiten an optischen Anzeigeeinheiten in Flachbauweise, ergonomische Anforderungen an Flachbildschirme”.

Diese beinhalten die Forderung nach:

- klarer Bildschirmaufteilung
- logischer Benutzerführung
- keine sich überdeckenden Fenster
- wenig Popup-Fenster für Parameterauswahl
- dem Einsatz gut lesbarer Schriftarten und –größen
- klarer und eindeutiger Symbole (Icon)
- dem sparsamen, aber wirkungsvollen Umgang mit Farben

Die auf dem Arbeitsplatzbildschirm ab 19“ Technik dargestellten Zeichen müssen deutlich, scharf und ausreichend groß (>5,3 mm) sein sowie einen angemessenen Zeichen- und Zeilenabstand besitzen.

Die Bedienoberflächen müssen eine schnelle und sichere Aufgabenbewältigung durch den Sachbearbeiter/Nutzer gewährleisten. Der Sachbearbeiter/Nutzer ist durch die Oberfläche sowohl in seiner Routinearbeit, aber auch bei größeren und kritischen Dateneingaben bzw. Ereignissen zu unterstützen. Das System soll dem Nutzer wesentliche Entscheidungen erleichtern. Dabei sind entsprechend der anstehenden Aufgabe nur die Programmpunkte, Funktionstasten, Menüpunkte, Befehlsschaltflächen und Listenfelder in den einzelnen Masken anzuordnen bzw. müssen angeordnet werden können, dass für die jeweilige Arbeitsaufgabe nur die erforderlichen und zugelassenen Befehlsreferenzen zur Verfügung stehen und so möglichst geringe Belastungen entstehen, wobei die Masken einheitlich aufzubauen sind. Eine kontextgeführte Bedienung und die Reduzierung der notwendigen Arbeitsschritte bzw. Mausklicks in der GUI werden gefordert. Eine Informationsflut auf dem Monitor des Nutzers ist unbedingt zu verhindern.

Strukturell zusammenhängende Daten sind in grafischer Form als Baumstruktur darzustellen. Die Bestimmung von Zuständigkeiten und Bereichsfolgen muss aus dem System heraus vorgenommen werden können.

Erweiterungen und Anpassungen der Masken und des Workflows müssen bis zu einem gewissen Grad von einem berechtigten Nutzerkreis bzw. der ZpIuK vorgenommen werden können, d. h. sie sind konfigurierbar zu gestalten.

Das WINDOWS-Regelwerk und die Bildschirmarbeitsverordnung, aufbauend auf der ISO 9241, einschließlich ihrer Spezifizierung (Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten, Teil 110: Grundsätze der Dialoggestaltung), sind zu beachten.

Die Bedienoberfläche muss weitestgehend selbsterklärend sein. Sie ist vollständig in der Amtssprache Deutsch zu realisieren.

6.1.2 Anforderungen an die Benutzerhilfe/-dokumentation

Eine umfassende Online-Hilfefunktion muss implementiert sein und von jedem Eingabefeld der Oberfläche aus, auch unabhängig von der Cursorposition, abrufbar sein (Direkthilfe).

Ein Benutzerhandbuch ist parallel zur Online-Hilfe zu erstellen, dabei ist die Norm VDI 4500 Blatt 1 „Technische Dokumentation – Benutzerinformation“ einzuhalten.

Die Benutzerdokumentation und die Hilfetexte müssen in der Amtssprache Deutsch vorliegen.

6.1.3 Anforderungen an die Benutzerführung

Die Benutzerführung in der Software muss sicherstellen:

- die Unterstützung des Nutzers in der Prozessbearbeitung durch das System, eine Bearbeitungsreihenfolge soll sichergestellt werden,
- die Information für Benutzer, bei welchem Prozess-Schritt er sich gerade befindet,
- dass Prozesse und Abläufe in eine oder mehreren Phasen unterteilt werden können, um die prozesskonforme Arbeit zu unterstützen und Abweichungen weitestgehend zu unterbinden, werden bestimmte Funktionalitäten nur in Abhängigkeit zur Phase (Prozess-Status) angeboten,
- dass Phasenübergänge mit Plausibilitätsprüfungen verbunden sind,
- dass Basisfunktionalitäten und Auskunftsdienste immer verfügbar sind, d. h. sie können zu jeder Zeit und unabhängig vom jeweiligen Prozess genutzt werden,
- dass “Zwischenspeichern“ des aktuellen Bearbeitungsstandes erfolgen kann,

- dass eine parallele Bearbeitung von mehreren Anliegen/Vorgängen möglich ist,
- dass Prozess-Phasen/Abläufe je nach Prozess variieren können,
- dass das System die Reihenfolge in der Bearbeitung sicherstellt,
- dass durch das System verhindert wird, dass unberechtigte Dritte Zugriff haben und Eingaben tätigen
- dass das System Aktionen unterbindet, die vom Prozessmanagement nicht vorgesehen sind,
- dass bei Aufruf von externen Systemen alle im System vorhandenen Daten an das externe System übergeben werden und dass Fehlfunktionen externer Systeme in der Anwendung abgefangen werden, ohne den weiteren Ablauf zu unterbinden.

Der Lieferant muss die zukünftigen Nutzer im Zuge des Customizing der Anwendung in das Design und die Herstellung einer gebrauchsfähigen Oberfläche involvieren und diesen Prozess dokumentieren.

6.2 Prinzip der Einmaleingabe und Mehrfachnutzung von Daten

Bei der Datenverarbeitung ist das Grundprinzip der Einmalerfassung und Mehrfachnutzung von Daten konsequent umzusetzen. Die in der Erfassungsmaske für Vorgänge eingegebenen Daten sind nach durch den Sachbearbeiter veranlassten Abfragen automatisch in entsprechende Abfragemasken zentraler Auskunftssysteme und in Bearbeitungsverfahren der Thüringer Polizei zu übernehmen. Zentrale Auskunftssysteme sind unter anderem:

- ComVor-Index
- INPOL
- EWO
- KBA-Verfahren wie ZFER, ZFZR, usw.
- AZR
- NWR
- ZIMP (geplant)

Gleiches gilt für Abfragen in anwendungsinternen Datenbanken bzw. für Datenübernahmen aus Quellsystemen.

6.3 Anforderungen an die Antwortzeiten und Performance

Die maximale Antwortzeit bei der Ausführung von Funktionen muss die fachlichen Anforderungen erfüllen. Spezifische Antwortzeiten werden im jeweiligen Fachkonzept gefordert. Diese sind im Rahmen der Abnahme durch den Leistungserbringer nachzuweisen.

Die GUI und NUI müssen ein flüssiges Arbeiten ermöglichen. Dies muss durch kurze Lade-, Speicher- und Latenzzeiten sichergestellt werden.

Sind keine speziellen Zeiten im Fachkonzept festgelegt, gilt als Mindestanforderung:

- Anmeldeprozesse in der Regel kleiner 10 Sekunden, max. 20 Sekunden,
- Aufbauzeiten von Bildschirminhalten in der Regel 1 Sekunden, max. 2 Sekunden,
- komplexe Suchanfragen innerhalb des Gesamtsystems in der Regel kleiner 10 Sekunden, max. 30 Sekunden,
- einfache Suchanfragen in der Regel 1 Sekunden, max. 4 Sekunden,
- Verarbeitung von Daten aus Systemen des ISTPOL in der Regel 5 Sekunden, max. 10 Sekunden,
- Druckausgaben innerhalb von in der Regel 7 Sekunden, max. 15 Sekunden.

Die Antwortzeiten sind bei Vollauslastung der Anwendung zu gewährleisten. In der Regel heißt, in min. 90 % der Fälle ist die Antwortzeit zu erfüllen.

6.4 Anforderungen an Standardausgaben

Die Ausgabe von Formularen, Listen und Rechercheergebnissen ist weiterverarbeitungsfähig in den Formaten von MS Office® (.docx, .xlsx) zu gewährleisten.

Die Ausgabe druckreifer Dokumente, die keiner Bearbeitung mehr bedürfen, muss schreibgeschützt im Portable-Document-Format (.pdf) erfolgen.

Als Standardaustauschformat werden auch .xml- und .csv-Dateien akzeptiert.

6.5 Anforderung an Protokollierung

Gemäß Fachkonzept sind einzelne Maßnahmen bzw. Änderungen an Daten lückenlos und beweissicher zu protokollieren.

Eine konfigurierbare, systeminterne Zugriffs- und Ergebnisprotokollierung ist umzusetzen.

Die Protokollierungsmöglichkeiten des IT-Verfahrens müssen revisionssicher sein. So muss nachträglich überprüft und festgestellt werden können, welche Daten zu welcher Zeit von wem in das Verfahren eingegeben, verändert und recherchiert worden sind (geeignete und den Anforderungen des Datenschutzes entsprechende Protokollierung in der Datenbank mit Auswertemöglichkeiten für berechtigte Nutzer).

6.6 Anforderungen an Profile

Welche spezifischen Profile und frei-gestaltbaren Nutzereinstellungen möglich sind, wird in den fachlichen Anforderungen beschrieben. Profildaten und Berechtigungen sind zentral in der Anwendung zu speichern. Das Anlegen von nutzerspezifischen Daten auf dem lokalen Arbeitsplatz des Anwenders ist auf ein Minimum zu begrenzen.

Servergestützte Profile des Clients werden im ISTPOL aktuell nicht genutzt. Sollte dazu ein Erfordernis bestehen, ist eine vorherige Absprache mit der ZpIuK erforderlich.

6.7 Servertechnik, Datenbanken, Applikationsserver, Arbeitsplatz

6.7.1 Server und vergleichbare Technik

Im Rahmen der Standardisierung des Betriebes sollten Synergieeffekte vorhandener Hardware und Verträge genutzt werden. Ebenfalls ist der Einsatz von Open Source basierenden Produkten mit verfügbaren Quelltexten und damit einhergehenden offenen Standards zu bevorzugen. Als Befehlssatz-Architektur dient vornehmlich x86 / x64. Es dürfen aber auch weitere Architekturen zum Einsatz kommen (z.B. ARM).

Diese muss folgenden Anforderungen entsprechen:

- Alle Bauteile und Komponenten für Systeme mit einer Verfügbarkeitsanforderung > 99,0% (VK1 und höher) sind redundant und wechselfähig vorzusehen (insbesondere Stromversorgung, Lüftertechnik, Switchtechnik für Ethernet).

- Sofern nicht spezifische Anforderungen gestellt werden, sind auf alle Teile der Lieferung Herstellergarantien von min. 2 Jahren vor Ort mit Reaktionszeit von max. 4 Stunden während der Arbeitszeit (Mo. – Fr. 07:00 – 16:00 Uhr) zu leisten. Die Erweiterung auf 5 Jahre ist anzubieten. Reparaturzeiten oder Umgehungen zur Wiederherstellung der Grundfunktionalität sind innerhalb 5 Arbeitstagen zu gewährleisten bzw. muss dem erforderlichen Schutzbedarf entsprechen.
- Der vorbeugende Austausch auf Grund möglicher Fehlerindikationen für Festplatten, Prozessoren, Hauptspeicher und Einschubkomponenten ist innerhalb von 3 Arbeitstagen zu leisten.
- Für alle Komponenten muss für mindestens 5 Jahre ab Inbetriebnahme die Ersatzteillieferung sowie für weitere 3 Jahre die Kompatibilität von Erweiterungskomponenten garantiert werden.
- Festplatten oder andere Datenträger verbleiben im Fehlerfall bei der Thüringer Polizei, dies ist in den Wartungsverträgen zu regeln.
- Rastermaß 19 Zoll Netzwerkschränktechnik ist grundsätzlich zu verwenden.
- Ein Update aller erforderlichen ROM, BIOS zum Auslieferungszeitpunkt auf aktuellem Stand ist auszuführen.
- Die kompletten Handbücher und Dokumentationen sind in gedruckter oder elektronischer Form zu liefern.
- Fehlermeldungen und MIB sind für die Managementsoftware (ICINGA®/NagVis® / WhatsUpGold) einzurichten bzw. zu übergeben.
- Eine Automatisierte Hot-Spare Funktion bei Ausfall einer Teilkomponente z. B. Festplatten oder Bladeserven ist vorzusehen.
- Die geregelte Stromversorgung hot-plug-fähig und redundant mit Stand-By-Betrieb für nicht benötigte Netzteile ist notwendig.
- Geregelte Lüfter hot-plug-fähig und redundant sind zu realisieren.
- Das Bonding/Teaming der anwendungsseitigen LAN-Netzwerkanschlüsse gemäß der Anforderung pro System wird gefordert.
- Ein separater Netzwerkanschluss zur Administration ist zu realisieren.

- Für die Gesamtheit der zu liefernden Technik wird ein uneingeschränkter Betrieb bei einer Toleranz der Luftfeuchte zwischen 20 % und 80 % (nicht kondensierend), im Temperaturbereich von 15 °C bis 30 °C sowie bei einer reinen Luftkühlung gefordert.
- Alle Aktivkomponenten im Bereich der Server-, Storagesysteme und zentraler aktiver Technik müssen SNMP mindestens in der Version 2 oder höher unterstützen.
- Es ist jeweils die aktuelle Gerätegeneration anzubieten und einzusetzen. Keines der Geräte und verwendeten Softwareversionen darf zum Zeitpunkt der Angebotsabgabe durch den Hersteller als "End-of-Life" klassifiziert oder angekündigt sein.
- Die Verwendung einer möglichst homogenen Geräteausstattung wird seitens der ZPIuK angestrebt. Bei Wahl der angebotenen Komponenten unter Beachtung wirtschaftlicher Kriterien und optimaler funktioneller Eignung soll nach Möglichkeit Technik eines Geräteherstellers verwendet werden.
- Für alle Geräte bzw. Hardwarekomponenten ist sicherzustellen, dass die Thüringer Polizei mindestens 5 Jahre kostenlos auf alle neuen Firmware-Releases (sowohl Major- als auch Minor-Releases) zugreifen und diese Versionen uneingeschränkt auf den gelieferten Geräten einsetzen darf.

6.7.2 Anforderungen an Hypervisor

Als Virtualisierungsplattform dienen vornehmlich VMWare als auch Linux KVM basierte Lösungen wie Proxmox.

6.7.3 Anforderungen an Betriebssysteme

Als UNIX basierte Betriebssysteme können grundsätzlich folgende Distributionen in der möglichst aktuellen oder Langzeit unterstützten Variante zum Einsatz kommen:

- ORACLE LINUX® (insbesondere für Oracle Datenbankserver)
- RedHat Linux®
- Debian
- armbian

Weiterhin sollten Produkte möglichst auf die am aktuellsten verfügbaren Kernel der Linux Foundation setzen.

Microsoft WINDOWS Server sind mindestens mit der Version 2019 Standard auszurüsten und in das AD zu integrieren.

Betriebssystemlizenzen für Server sind durch den Lieferanten zu berücksichtigen und in den Angebotskalkulationen aufzunehmen. In Absprache mit der ZpIuK können BS-Lizenzen über die Rahmenverträge des Freistaates oder des Bundes beigestellt werden.

Abweichungen von den beschriebenen Vorgaben sind mit dem Auftraggeber abzustimmen und durch diesen zu genehmigen.

6.7.4 Anforderungen an Datenbanken

Derzeit sind verschiedene Versionen von ORACLE®-DBMS in der Thüringer Polizei im Einsatz. Eine Vereinheitlichung der Versionierung wird angestrebt. Für neue Verfahren gilt:

1.) für hochverfügbare Datenbanken: (Systeme mit Verfügbarkeitsanforderung VK2-VK5 nach BSI HV-Kompendium)

- ORACLE® Datenbank Vers. 19.x
- im 2 Node RAC mit Kompatibilitätsmodus zu 18.x,
- Datenbank Server unter ORACLE LINUX® auf x86-64 Architektur

Die Datenbank-Lizenz wird durch eine nutzerbasierende ORACLE Lizenz durch die ZpIuK bereitgestellt.

2.) für sonstige Datenbanken: (Systeme mit Verfügbarkeitsanforderung VK0 und VK1)

a. ORACLE® Datenbank Vers. 19.x mit Kompatibilitätsmodus zu 18.x, Datenbank Server unter ORACLE LINUX® auf x86-64 Architektur, nicht virtualisiert

Die Datenbank Lizenz wird durch eine nutzerbasierende ORACLE Lizenz durch die ZpIuK bereitgestellt.

b. MS-SQL® Datenbank unter MS Server 2019® oder höher auf x86-64 Architektur

MS-SQL® Datenbanklizenzen sind durch den Lieferanten zu kalkulieren.

Auch die ORACLE®-Support Produkte wie z. B. Partitioning, Diagnostics Pack, Tuning Pack, Configuration Management Pack for ORACLE Database, Diagnostics Pack for ORACLE Middleware, WebLogic Server Management Pack Enterprise Edition (ORACLE-WLS®) werden durch die ZpIuK bereitgestellt.

Als Zeichensatz auf Schnittstellen, der Dateneingabe, in der Datenbank und in der Anwendung ist DIN 91479 (String.Latin+ 1.2) gem. Entscheidung des IT-Planungsrates (2019/16) zwingend zu implementieren.

6.7.5 Anforderungen an Applikations- / Webserver

Für die Anwendungsserver gilt:

1.) für hochverfügbare Anwendungsserver (Systeme mit Verfügbarkeitsanforderung VK2-VK5)

Es ist ein redundanter Applikationsserver mit vorgeschaltetem Loadbalancer einzusetzen. Vorzugsweise wird dieser auf einem der benannten Linux basierten Betriebssysteme betrieben.

2.) Nicht hochverfügbare Anwendungsserver: (Verfügbarkeit VK0 und VK1)

Es kann ein Applikationsserver als alleinstehende Instanz betrieben werden. Redundanzen der Dienste sind optional.

Als Webserver kommt auf UNIX basierten Betriebssystemen vorzugsweise folgende Software zum Einsatz:

- Apache Webserver
- Nginx
- Internet Information Server für integrierte Microsoft WINDOWS Webapplikationen

Die Thüringer Polizei besitzt eine EAI/Servicebus Infrastruktur basierend auf dem Interface Manager der Fa. T-Systems. Schnittstellen werden sowohl in EAI/Konnektoren Technologie wie auch Punkt-zu-Punkt realisiert. Dies trifft jedoch nur bei wenigen Einzelverfahren zu.

6.7.6 Arbeitsplätze

In der Thüringer Polizei werden PCs und Notebooks als Endgeräte eingesetzt.

Als Monitore für PC‘s sind min. 24’’-Geräte bei Neubeschaffungen Standard. Die Mindest-Bildschirmauflösung für die Endgeräte der Thüringer Polizei beträgt derzeit 1920 x 1080. Sollte im spezifischen Lastenheft/Leistungsbeschreibung nichts geregelt sein, müssen Arbeitsplatzgeräte (PC, Notebooks, Monitore) mind. eine Full-HD Auflösung mit 1920 x 1080 Bildpunkten aufweisen.

Als Zielplattform für Anwendungen im ISTPOL ist aktuell ein Standard PC auf X86 Technologie mit einer Prozessorleistung von größer 2,4 GHz, größer 8 GB RAM mit Betriebssystem als Mindestausstattung vorauszusetzen.

Auf dem Client ist zurzeit der ORACLE® Client und die aktuelle Java® Runtime Environment ausgerollt.

Der durch den Betrieb von Visualisierungsgeräten, Druckern, Clients und zugehöriger Technik im Umfeld der Nutzer verursachte Schalldruckpegel darf unter Freifeldbedingungen in einem Abstand von 3m einen Wert von 25 dB(A) einschl. eines ggf. in Ansatz zu bringenden Tonzuschlages gem. der Norm DIN 45681 "Akustik - Bestimmung der Tonhaltigkeit von Geräuschen und Ermittlung eines Tonzuschlages für die Beurteilung von Geräuschimmissionen" nicht überschreiten. Die VDI Richtlinie 2569 „Schallschutz und akustische Gestaltung im Büro“ ist einzuhalten.

6.7.7 Virtuelle Desktop-Infrastruktur (VDI)

Die Thüringer Polizei besitzt eine VDI-Infrastruktur basierend auf CITRIX Software, wobei die Clients innerhalb vorhandener VMware/ESX-Umgebungen gehostet werden. Als Hypervisor für VDI-Clients ist zwingend CITRIX einzusetzen.

6.7.8 Technologiestandards

Zur Vereinheitlichung der IT-Verfahren der Polizeien der Länder und des Bundes wurde ein auf SAGA 5.0 aufbauender Standard definiert und zwischen den Ländern abgestimmt.

Bei Webanwendungen muss das neue Produkt eine vom Browsertyp unabhängige Anwendung sein. Bei Bedarf ist vorzugsweise Java-Technologie einzusetzen.

Zusätzliche Standards sind im Dokument „Technologien, Standards, Protokolle, Architekturen“ (TSPA), Version 1.3 der Thüringer Landesverwaltung formuliert. Der Einsatz von offenen Standards / Technologien ist erwünscht.

6.8 Sonstige Technik/Räumlichkeiten

Produktivumgebungen für neu einzuführende zentrale Verfahren werden grundsätzlich im TLRZ aufgesetzt. Die Systeme der DMZ, Firewall sowie Test- und Entwicklungsumgebungen werden am Technikstandort TLKA betrieben.

Die Serverräume sind meist nicht ebenerdig erreichbar. Die Nutzung eines Fahrstuhls oder Lastenaufzug ist nicht an allen Standorten sichergestellt. Es wird empfohlen, vor Aufstellung der Technik die entsprechenden Zugänge zu den Technikräumen durch den Lieferanten zu klären.

Die Installation zentraler Technik soll in vorhandene 19“-Schränke (Beistellleistung der ZpIuK) erfolgen, diese haben folgende Eigenschaften:

- Sie werden auf Doppelböden aufgestellt.
- Sie besitzen eine Kabeleinführung von unten.
- Sie besitzen eine Tiefe von 1200 mm, Breite von 800 mm, Höhe von 2000 mm.
- Kabelanschlüsse/Patchfelder sind überwiegend rückseitig ausgeführt.
- Sie besitzen max. 41 Höheneinheiten (HE).
- In jedem Serverschrank soll eine Platzreserve von 30 % für spätere Nachrüstungen verbleiben.
- Die Anordnung der geräteinternen Lüfter/Luftrichtung unter Beachtung der Anordnung „Kaltgang“ ist gefordert.
- In den Serverschränken ist keine Brandfrüherkennung vorhanden. Der Serverraum und der Warmbereich sind mit automatischen Brandmeldern ausgestattet.
- Bauseitig sind die Schränke mit Stromversorgungsverteilern (PDU-Schienen) ausgerüstet. Die maximale Lastabnahme, respektive Kühlleistung pro Schrank beträgt max. 10 KW oder 45 A 230V~. Erwartet werden Netzanschlüsse 230V~ max. 16A je Anschluss (1 Phase) mit C19 Anschlüssen für Blade Systeme oder Kaltgeräte Steckern für Standard Systeme.

- In der Regel verfügen die Schränke in den rückseitigen, oberen 6 HE über Patchfelder zum Anschluss der Netzwerk-Verbindungen.
- Sofern im Leistungsverzeichnis nichts anders geregelt ist, sind sämtliche Geräte in Serverräumen mit redundanten Netzteilen bzw. mit PowerSwitchTechnik auszustatten.

Die Stromversorgung erfolgt über die Netzverteilung des Hauses/Rechenzentrums. Diese ist durch eine entsprechende Notstromersatzanlage (NEA) abgesichert. Die Überbrückung der Zeit vom Stromausfall bis zum Betrieb der NEA wird über USV abgesichert. Für den Ausfall der Netzersatzanlage ist eine Prozedur zu implementieren, welche durch ein Scripting mittels ICINGA®/NagVis® ein kontrolliertes und sicheres Herunterfahren sämtlicher Technik innerhalb von max. 15 min. nach Auslösen des Scripts ermöglicht.

Der Betrieb zentraler Technik erfolgt in einem gekühlten Raum (in der Regel einheitliche Umgebungstemperatur).

Sofern der Auftragnehmer Technik installiert, sind die LAN- und FC-Anschlusskabel nach der Beschriftungsrichtlinie der ZpIuK durch den Auftragnehmer zu beschriften.

6.9 Anforderungen an Administration und Monitoring

Die Administration der Anwendung betrifft:

- die Implementierung einer Systemstörungsüberwachung mit NAGIOS/ICINGA®
- das Prozessmonitoring mit NAGIOS/ICINGA®
- die grafische Systemdarstellung mit NagVis®
- den Neustart von Systemdiensten, Systemen und Prozessen mittels NAGIOS/ICINGA®
- die Anpassung des Systems auf die konkrete IT-Umgebung
- die Vergabe und Pflege von Gruppen-Zugriffsrechten, Profilen
- das Einrichten/Anpassen der Anwendung
- das Einrichten/Anpassen der Anwenderoberfläche (Logos, Masken Layout etc.)
- den Zugriff auf die Protokolldateien
- die Pflege und Freigabe von Katalogen

Für die Administration wird eine browserorientierte Nutzerschnittstelle (HTML5-Technologie) erwartet. Der Zugang zu dieser Nutzerschnittstelle ist einer Administrationsgruppe vorbehalten. Diese Gruppe soll unabhängig von Systemadministrationsrechten des Betriebssystems die volle Administration der jeweiligen Anwendung ermöglichen. Die Integration der Anwendung in das NAGIOS/ICINGA®/NagVis® Monitoring System und die Unterstützung der ITIL-basierenden Service Management Prozesse ist zwingend zu realisieren.

Ein Berechtigungskonzept muss die Anforderungen abbilden.

An die Administration und Management der Lösung werden folgende spezielle Anforderungen gestellt:

- Die Systeme/Anwendungen müssen sich remote steuern, starten und konfigurieren lassen. (z. B. Remotemanagement ILO der Fa. HP) mittels:
  I. Remote Konsole über klassische Shell
  II. Remote Konsole über Webbrowser
- Die Lösung soll die interaktive Konfiguration, Performanceauswertung/Tuning und Administration über GUI und/oder Web-Interface unterstützen, die in der täglichen Anwendung einfach zu benutzen und ohne Einfluss (z. B. Downtime) auf die Applikationen ist.
- Die Admin.-GUI oder –Web-Interface ist in Deutsch, optional Englisch auszuführen.
- Die Technik muss Statusinformation und Störungsmeldungen an das Managementsystem über SNMP und Logfiles (incl. MIB für SNMP-Anbindung an NAGIOS/ICINGA®/NagVis®) übergeben.
- Die Anbindung von Hardware an HP-SIM (HP-SIM Server im TLKA vorhanden) muss erfolgen.
- IT-Grundschutzanforderungen an die Informationssicherheit sind für die Administration umzusetzen. Dazu zählt im Besonderen:
  I. Eine Nachvollziehbarkeit der Administrationstätigkeiten in Logfiles wird gefordert.
  II. Authentifizierung über SSO gegen AD-Server via AD Usergruppen ist zu realisieren.
  III. Die generelle Eignung der Lösung gemäß BSI Sicherheitsstandards 200-1 bis 200-4 ist inklusive der Umsetzung herzustellen.

6.10 Anforderungen an die Virtualisierung

Die Komponenten neu einzuführender Verfahren müssen auf die Vorteile einer Virtualisierung geprüft werden. Sollte keine Virtualisierung zum Einsatz kommen, ist dies durch den Lieferanten des Systems zu begründen.

Als grundsätzlich zu nutzende Virtualisierungssoftware für Anwendungen wurde VMware® festgelegt, wobei im Microsoft®-Umfeld für Infrastrukturdienste auch die Nutzung von HyperV® möglich ist. Sollten neue IT-Verfahren die Verwendung einer spezifischen Virtualisierungstechnologie vorschreiben, ist dies durch den Hersteller explizit zu begründen.

6.11 Anforderungen an Clustering und Hochverfügbarkeit

Hochverfügbare zentrale Verfahren werden als Clusterlösungen bzw. im Parallelbetrieb mit Loadbalancer betrieben.

Für Datenbanken wird ORACLE® RAC Technologie genutzt.

IT-Architekturen für neue Verfahren sind an einer effizienten Auslastung der Hardware auszurichten - passive Hardwarelösungen (warm/cold standby) sind zu vermeiden.

Die theoretische Verfügbarkeit des Verfahrens hat der Lieferant auf Basis der Einzelverfügbarkeiten (Infrastruktur, Netz, Hardware, Datenbank, Services, Prozesse etc.) gemäß anerkannter Normen und Standards (DIN/VDI) nachzuweisen.

6.12 Anforderungen an die Benutzerverwaltung

Die Berechtigungsdaten der Nutzer werden im AD hinterlegt und sollen dort zentral gepflegt werden. Dafür werden verfahrensspezifische Benutzergruppen im AD angelegt und Nutzer diesen Gruppen zugeordnet. In den Verfahren sollen nur Benutzerprofile mit den zugehörigen Rechten mit Bezug zu den Benutzergruppen des AD definiert werden.

Vorzugsweise sind hierfür AD-/ADFS- oder LDAP-Schnittstellen zu realisieren.

Zusätzlich ist im Verfahren eine rudimentäre eigene Nutzerverwaltung zu implementieren, diese dient für spezielle Berechtigungen (z. B. Testuser), Pilotierung und Rückfallszenarien bei Nichterreichbarkeit des AD.

6.13 Implementierung Single-Sign-On

Neu einzuführende Verfahren müssen generell Single-Sign-On via Kerberos-Authentifizierung gegen das AD unterstützen.

6.14 Werkzeuge, FLOSS-Produkte, zusätzliche Lizenzen

Die Nutzung und Freigabe von lizenzpflichtigen Produkten ist mit der ZpIuK generell abzustimmen.

Falls der Lieferant eines Systems bzw. Verfahrens lizenz- bzw. urheberrechtlich geschützte Softwaremodule, Halbzeuge bzw. Entwicklungswerkzeuge anderer Hersteller einsetzt oder Free/Libre Open Source Software (FLOSS) zum Einsatz kommt, ist die schriftliche Zustimmung durch die ZpIuK im Vorfeld des Einsatzes erforderlich.

Eine Auflistung der benötigten bzw. der von Lieferanten verwendeten Werkzeuge, SW-Komponenten und Systeme ist dem Angebot beizufügen. Geforderte Beistellleistungen der ZpIuK sind auszuweisen.

6.15 Kataloge

Neu einzuführende Verfahren müssen generell die vorhandenen, zentral gepflegten Katalogwerte nutzen, für verfahrensspezifische Kataloge ist im Vorfeld die Zustimmung der ZpIuK erforderlich.

6.16 Anforderungen an die Softwareverteilung

Für FAT-Clients ist durch den Hersteller der Software die unbeaufsichtigte und automatische Softwareverteilung durch MECM® zuzusichern.

6.17 Anforderungen an die Software

Software sollte sich im Grundsatz an den qualitativen Merkmalen der ISO-25010/9126 orientieren, wobei sich das Augenmerk auf Folgende konzentriert:

- einfache Handhabung

- leichte Erlernbarkeit durch nicht geschultes Personal
- Fehlerbhandlung von Interaktionsfehlern durch Benutzer
- Wahrung der IT-Sicherheit als Unterrubrik der Informationssicherheit durch Einhaltung von Integrität (Datenintegrität), Authentizität, Verfügbarkeit und Vertraulichkeit
- Portierbarkeit zwischen verschiedenen Betriebssystemen innerhalb einer Architektur (insbesondere Linux / Windows x86)

Der Einsatz Open-Source basierter Software ist zu bevorzugen.

6.17.1 Anforderungen an die Softwarearchitektur

Für die Datenverarbeitung gilt der Grundsatz der Einmaleingabe und Mehrfachnutzung von Daten.

Redundante Dateninhalte sind in Verfahren so zu halten, dass regelmäßig (synchron od. asynchron) die Daten mit dem führenden System abgeglichen werden können.

Die Software ist modular aufzubauen. Systeme müssen bei Ausfall einzelner Komponenten autark sein und automatisch die Verbindung und Funktionalität wiederaufbauen.

Als Zeichensatz ist durchgängig DIN 91479 (String.Latin+ 1.2) gem. Entscheidung des IT-Planungsrates (2019/16) zu verwenden.

Datenstrukturen in der Anwendung und auf den Schnittstellen müssen zum XPolizei-Standard, im Besondern zum Informations- und Datenmodell der Polizei (IMP) in der aktuellen Version kompatibel sein.

Ausfall oder Fehler in Schnittstellen oder Störungen externer Services sind durch Fehlerroutinen in der Anwendung zu behandeln. Bei Auswirkungen auf Abläufe und Funktionen der Anwender sind Fehlermitteilungen in für den Nutzer verständlicher Form darzustellen.

Auf die Verwertung, Mehrfachnutzung und Synergien von vorhandenen Lizenzen des ISTPOL gemäß Kapitel 3.2 wird verwiesen.

Unten aufgeführte IT Basisdienste sind zu verwenden, das gilt im Besonderen für zentrale Services, wie Netzdienste, Servicemanagement, Infrastrukturdienste, Katalogwerte etc.

Lfd. Nummer	Abkürzung	Basisdienst / Erläuterung	zu verwendende Produkte
1	ADS/ADDS	Active Directory Services/Active Directory Domain Services Zentraler Verzeichnisdienst je nach Serverversion inkl. Global Catalog Server und Single Sign On Elektronisches Telefonbuch	Windows Server Active Directory Dienste
2	DHCP	Dynamic Host Configuration Protocol	Windows Server DHCP Dienste inkl. DHCP Relays in den Routern
3	DNS	Domain Name System Zur Namensauflösung im ISTPOL (AD integriert)	Windows Server DNS-Dienste
4	SDS/SPS/ SUS	Software Deployment Service/ Software Provisioning Service/ Software Update Service Softwareverteilserver für heterogene Umgebungen	MECM
5	NMS	Network Management System	NAGIOS/ICINGA® / NagVis® Monitoring
6	Monitoring	Systemüberwachung mit Schwellwertalarmierung	NAGIOS/ICINGA® / NagVis® Monitoring
7	KLB	Knowledgebase	Omnitracker

Lfd. Nummer	Abkürzung	Basisdienst / Erläuterung	zu verwendende Produkte
8	UHD	User Help Desk	Omnitracker
9	TTS	Trouble Ticket System	Omnitracker
10	NTP	Network Time Protocol Server Zeitsynchronisation für alle Systeme	Lantime NTP-Server
11	AVS	Antivirus System Servergestütztes Antivirussystem mit automatischem Update der Virenpattern	MS Defender
12	Backup	Backup-System Servergestütztes Backup-System mit Backupclients und -agents für verschiedene Betriebssysteme und Applikationen	HP Dataprotector
13	SM	Storage Management zur Verwaltung des zentralen Storage	HP-SM für HP EVA, P2000 und 3PAR Lösungen.
14	DBS	Datenbanksystem	ORACLE Incl. DB- Management Tools
15	VDI	Virtual Desktop-Infrastruktur	CITRIX mit Client Betrieb
16	CMDB	ITIL konforme Konfigurationsdatenbank	Omnitracker

6.17.2 Umgang mit Schnittstellen

Schnittstellen bilden in der Regel komplexe Datenströme ab und sind daher oft Ursache für Fehler bzw. Nachbesserungen.

Daher hat ein Lieferant von Verfahren für Schnittstellen seines Systems eine Schnittstellenbeschreibung in Form einer Schnittstellenvereinbarung/System Interface Agreement (SIA) zu erstellen bzw. zu überarbeiten. Diese beinhaltet:

- die grundlegende Beschreibung der Schnittstelle
- fachliche Abläufe
- Datenfelder, Identifikation, Syntax, Mapping und Austauschkriterien
- technische und organisatorische Abläufe innerhalb der Schnittstelle
- fachliches Verhalten zu spezifischen Störungen, insbesondere Wiederanlauf, Synchronisation, Dateninkonsistenzen
- betriebliche Themen und Vereinbarungen:
    - Überwachung und Betriebsinformation zur Schnittstelle
    - Rollenangaben der beteiligten Systeme
    - fachliche und technische Ansprechpartner für die beteiligten Systeme
    - Kommunikation zwischen den beteiligten Rollen
    - Prozessbeschreibungen
    - Incident Management
    - Change Management
    - SLA - Monitoring und -Steuerung
    - Eskalationsverfahren
    - generelle Verfügbarkeit der beteiligten Systeme
    - Wartungsfenster und sonstige Ausfallzeiten
    - Servicezeiten der beteiligten Systeme
    - Reaktions- und Wiederherstellzeiten
- Technische Vereinbarungen:

  - Datenvolumen
  - Mengengerüst
- Kennwerte bei Online-Schnittstellen:
  - Antwortzeitverhalten
  - Transaktionsrate
  - Durchsatz
- Kennwerte bei Offline-Schnittstellen
- Sicherheitsbezogene Vereinbarungen:
  - Klassifizierung der Daten der Schnittstelle
  - Datenschutz
  - Datensicherheit (Verfügbarkeit, Integrität, Vertraulichkeit)
  - Weitergabe von Daten an Dritte (indirekte Schnittstellen)
  - Aufbewahrungsdauer (Protokolle)
  - sonstige Anforderungen aus rechtlichen Rahmenbedingungen.
  - Kommunikationsplan (Port + Protokoll)

Ein SIA ist von der jeweiligen Betriebsverantwortung (BV) der beteiligten Systeme zu unterzeichnen.

6.18 Bereitstellung und Nutzung von Geoinformationen

Die Thüringer Polizei betreibt eine eigenständige Geodateninfrastruktur (GDI-TH-Pol) nach den Vorgaben des Architekturkonzeptes der GDI-DE. Diese Infrastruktur stellt für die Polizei des Freistaates Thüringen zentral Geodaten, Geodienste und -services sowie Metadaten bereit.

Wird von der zukünftigen Lösung eine Bereitstellung oder Nutzung von Geodaten, Geodiensten, Metadaten oder Geoservices gefordert, sind hierbei die Daten und Funktionalitäten der GDI-TH-Pol über eine GDI-konforme Schnittstelle zwingend zu nutzen. Eine Interoperabilität zwischen der Lösung und der GDI-TH-Pol ist vollumfänglich sicherzustellen.

Für die Einbindung der durch die GDI-TH-Pol bereitgestellten Daten und Dienste in die Lösung sowie die Integration in die graphischen Benutzeroberflächen ist der Lieferant der Lösung verantwortlich (z. B. Bereitstellung von Eingabefeldern, Integration von Darstellungsdiensten etc.).

Kartendaten und zugehörige Lizenzen werden somit von der GDI-TH-Pol für alle Anwendungen bereitgestellt.

6.19 Anforderungen an Netztechnik, Netzwerkbandbreiten und Netzübergänge

Es gelten die unter Punkt 3.4 getroffenen Aussagen. Die Netzwerkbelastung durch eine Anwendung ist auf ein Mindestmaß zu beschränken. Durch den Lieferanten eines neuen Verfahrens sind die Auswirkungen auf das Netzwerk durch das Verfahren zu analysieren und darzustellen (Netzwerk Impact Analyse).

Netzanschlüsse in Technikzentren bzw. Serverräumen sind in u. g. logisch getrennten LAN's auszuführen:

- Produktion/Schulung/Referenz
- Administration
- Backup
- Interconnect

Die WAN MTU Size 1380 ist zu beachten. Das Verhalten der eingesetzten Layer- 3 Switche beim Erhalt von Paketen, die die MTU Size der WAN GRE Tunnel überschreiten, ist zu beachten. Eine feste Einstellung einer MTU Size kleiner als die WAN MTU Size 1380 kann für Clients oder Server notwendig sein.

Netzkomponenten sollen das Protokoll SNMP mindestens in Version 2c unterstützen.

Optional sind für Testzwecke separate LAN Strukturen zu realisieren.

Es muss sowohl das Protokoll IP Version 4 wie auch Version 6 unterstützt werden.

Schnittstellen mit Netzübergängen sind über das vorhandene Firewallsystem zu führen. Ist dies nicht möglich, ist die Konzeption einer entsprechenden Erweiterung des Firewallsystems Bestandteil der angebotenen Lösung.

Ein direkter Zugang ins Internet ist ausgeschlossen. Sind Internetzugriffe unbedingt notwendig, ist ein Transfersystem, das in einer DMZ platziert wird, Bestandteil der angebotenen Lösung.

6.20 Anforderungen an die Dokumentation

Die Lösung (Verfahren, Services und Systeme) ist entsprechend der einschlägigen Normen und Standards zu dokumentieren.

Die ZpIuK hat Vorgaben für die Dokumentation von Informationssicherheits- und Berechtigungskonzept sowie Benutzer- und Betriebshandbuch in einer Freigaberichtlinie definiert. Diese Standards sind grundsätzlich zu nutzen.

Software und Anpassungen an der Konfiguration sind durchgängig zu dokumentieren, d. h. in Handbüchern, Customizing-Logs, Programmierrichtlinien etc. Der Programmcode ist innerhalb der Programmierung und in UML 2.0 Diagrammen so zu dokumentieren, dass bei Übergabe des Quellcodes eine Weiterverarbeitung durch fachkundige Dritte möglich ist.

6.21 Anforderungen an die Verfügbarkeit

Anforderungen an die Verfügbarkeit werden in der Schutzbedarfsfeststellung durch den fachlichen Bedarfsträger erhoben. Dabei wird sich an den Regelungen und Empfehlungen des BSI zu Hochverfügbarkeitslösungen orientiert.

Sollte im Lastenheft oder der Leistungsbeschreibung keine Anforderung gestellt sein, sind mindestens Verfügbarkeiten von VK1 gemessen im Jahresmittel und maximale Wiederherstellzeiten von 5 Arbeitstagen zu realisieren.

6.22 Anforderungen an Datenschutz, -integrität und Informationssicherheit

Für die Informationssicherheit richtet sich die Thüringer Polizei nach den Empfehlungen des BSI. Als Anforderung gilt dabei insbesondere die Umsetzung der Anforderungen aus dem IT-Grundschutz-Kompendium des BSI in der jeweils gültigen Fassung.

Aus diesem Grund ist eine detaillierte Ermittlung des Schutzbedarfs durch den Bedarfsträger nach Empfehlungen des BSI erforderlich. Vom Ergebnis der Schutzbedarfsfeststellung sind die für den technischen Betrieb erforderlichen Maßnahmen durch den Lieferanten umzusetzen.

In Anlehnung an §54 ThürDSG *„Anforderungen an die Sicherheit der Datenverarbeitung“* ist über die Implementierung von erforderlichen technischen und organisatorischen Maßnahmen hinaus ebenfalls eine geeignete Dokumentation dieser durch den Anbieter im Zuge der Realisierung vorzusehen, sodass die Erstellung eines Informationssicherheitskonzeptes durch die zuständige Stelle gewährleistet werden kann.

Diese Maßnahmen müssen dazu geeignet sein, den Schutz der personenbezogenen Daten zu gewährleisten. Hierbei ist insbesondere durch geeignete technische Maßnahmen sicherzustellen, dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Gewährleistung der Vertraulichkeit),
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Gewährleistung der Integrität),
- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Gewährleistung der Verfügbarkeit),
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Gewährleistung der Authentizität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Gewährleistung der Revisionsfähigkeit),
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Gewährleistung der Transparenz).

Die Wirksamkeit dieser Maßnahmen ist durch den Anbieter unter Berücksichtigung der beschriebenen Rahmenbedingungen in der Thüringer Polizei und des Standes der Technik nachzuweisen. Notwendige Anpassungen, die sich aus einer späteren Änderung der Rahmenbedingungen in der Thüringer Polizei oder des Standes der Technik ergeben, sind durch den Anbieter nach Anforderung zeitnah zu realisieren.

Notwendige organisatorische Maßnahmen, die zur Erreichung der o. g. Sicherheitsziele durch den Bedarfsträger umgesetzt werden müssen, sind durch den Anbieter ebenfalls zu beschreiben.

Das angebotene Verfahren ist so zu gestalten, dass das oben beschriebene Informationssicherheitsniveau in der Thüringer Polizei aufrechterhalten werden kann und dass es einer späteren Zertifizierbarkeit der Thüringer Polizei nach ISO 27001 auf der Basis der Empfehlungen des BSI (Umsetzung entsprechend des ermittelten Schutzbedarfs) nicht entgegensteht. Die Standards des BSI 200-1 bis 200-4 sind einzuhalten.

Auch bei Outsourcing von Basisdiensten verbleibt die Steuerung, grundsätzliche Entscheidungen zu Technik und Wartung, der Applikationsbetrieb, der 24/7 Servicedesk und fachliche Betrieb in der ZpluK. Aus diesem Grund ist es erforderlich, dass neu einzuführende Verfahren eine revisionssichere Trennung von Basis- und Verfahrensadministration ermöglichen.

Durch den Anbieter eines neu einzuführenden Verfahrens sind auf der Grundlage der im Fachkonzept beschriebenen Anforderung und der Schutzbedarfsfeststellung ein Datensicherungskonzept (Backup- und Recovery-Konzept) und ein Notfallvorsorgekonzept für den Wiederanlauf des Verfahrens sowie ein Wiederanlauf-/ Wiederherstellungsplan gemäß BSI Standard 200-4 vorzulegen. In diesen Dokumenten sind erforderliche Arbeiten konkreten Rollen zuzuweisen. Die Notfallkonzeption beginnt auf der zu enthaltenen Risikoanalyse (BSI Standard 200-3).

Besonderer Wert wird auf die Zugriffsrechteverwaltung, -kontrolle und -protokollierung (siehe Sicherheitsrichtlinie für die Protokollierung im Informationssystem der Thüringer Polizei) in neu einzuführenden Verfahren gelegt.

Der Identifikations- und Authentifikationsmechanismus des Verfahrens muss nach den Vorgaben der Thüringer Polizei (siehe QM-Dokument QM-000-RL-0158) gestaltet sein. Ein Benutzer muss eindeutig identifiziert und authentifiziert werden können. Neben der Authentifizierung sind Mechanismen zur abgestuften Autorisierung von Nutzern erforderlich. Dabei ist die Nutzung der für alle Verfahren der Thüringer Polizei gültigen, eineindeutigen Anmeldenamen (Identifikationsnummern, 8-stellig, alphanumerisch) verbindlich.

Vor der Übertragung von Nutzer- oder Verfahrensdaten muss der Kommunikationspartner (Rechner, Prozess oder Benutzer) eindeutig identifiziert und authentifiziert sein.

Ein einzuführendes Verfahren muss die Umsetzung der Sicherheitspolitik der Thüringer Polizei ermöglichen, indem für jeden Benutzer die entsprechenden Sicherheitseinstellungen gewählt werden können.

Wenn die Anmeldung nicht über SSO erfolgt, sind die Anmeldeprozeduren so zu gestalteten, dass nur eine Passwortgüte nach dem Stand der Technik und den Empfehlungen des BSI möglich ist.

Fernwartungszugänge bedürfen einer genauen Beschreibung der Kommunikationsbeziehungen und einer Risikoanalyse im jeweiligen Informationssicherheitskonzept gemäß BSI – Standard 200-3.

6.23 Anforderungen an das Qualitätsmanagement des Anbieters

Es wird vorausgesetzt, dass die Entwicklung der Software beim Anbieter unter Beachtung gängiger Qualitätsstandards erfolgt.

Eine Zertifizierung des Anbieters nach ISO 9001:2015 wird als eine mögliche Dokumentation seines Qualitätsmanagements gewertet. Eine Zertifizierung des angebotenen Verfahrens vom BSI wird als positiver Bestandteil zum sicheren IT-Betrieb des Verfahrens gewertet, da sich die Thüringer Polizei nach den Empfehlungen des BSI richtet.

Die revisionssichere Archivierung bzw. fristgerechte Aussonderung von Daten ist in der Software mittels automatischer Routinen zu implementieren.

Für die aus dem ISTPOL heraus genutzten Verfahren und Schnittstellen von Dritten gelten deren Sicherheits-, Nutzungs- und Betriebsanforderungen in der jeweils gültigen Fassung.

7 Mengengerüst

Neben den beschriebenen Voraussetzungen in Bezug auf die vorhandene IT-Struktur der Thüringer Polizei sowie die Leistungsfähigkeit des Datenbanksystems und der zur Verfügung stehenden Bandbreiten ist für den Betrieb des Verfahrens noch von den folgenden quantitativen Angaben auszugehen:

Im ISTPOL arbeiten derzeit insgesamt etwa 6000 Nutzer mit den verschiedensten Kombinationen der Nutzungsrechte für die angebotenen Verfahren.

Die Nutzerzahlen für einzelne Verfahren sind unterschiedlich.

Ein detailliertes Mengengerüst für ein neu einzuführendes Verfahren wird durch den Bedarfsträger im Fachkonzept aufgestellt.

8 Betrieb, Servicemanagement (SM) / Wartung- und Support

Ein ITIL – basiertes Incident- und Changemanagement sind im ISTPOL implementiert. Der Lieferant muss sich mit seinem Integrations- und Supportprozess daran orientieren.

Neue Verfahren, Services und Produkte im ISTPOL dürfen erst nach Freigabe durch das TLKA in seiner Funktion als ZpIuK - entsprechend der geltenden Freigaberichtlinie in den Produktivbetrieb überführt werden. Durch den Anbieter sind dafür die Dokumentation über die implementierten Maßnahmen (siehe Kapitel 6.22) und ein Betriebshandbuch (BHB) für den gelieferten Umfang seiner Leistungen zu erstellen. Im BHB sind detailliert ein logisches- und physikalisches Systemdesign, die regelmäßigen Service- und Wartungstätigkeiten, Handlungsanleitungen für betriebliche Fehlerszenarien und die Anleitung zur Installation zu beschreiben. Die ZpIuK stellt dazu das Inhaltsverzeichnis und ein Template zur Verfügung.

Für Verfahren im Betrieb gilt der Änderungsprozess nach ITIL (d. h. Änderungen bedürfen einer formellen Freigabe durch den Änderungsbeirat der ZpIuK). Zudem gelten standardisierte Service Level Regelungen und Störungsklassen nach dem geltenden Servicekatalog.

In der Ausschreibungsphase, spätestens zur Einführung werden detaillierte bzw. höherwertige Service Level Agreements (SLAs) im Betriebshandbuch und ggf. im abzuschließenden Wartungsvertrag definiert.

Sollten für Supporttätigkeiten der ZpIuK besondere Qualifizierungen/Zertifizierungen des Personals erforderlich sein, muss ein Lieferant diese Rahmenbedingungen in seinem Angebot beschreiben.

Für die Wartung und den Support gilt im Besonderen:

- interne Datenträger vorhandener HW verbleiben im Fehler- bzw. Störfall beim Auftraggeber
- Störungsabläufe sind qualifiziert zu dokumentieren

Abkürzungsverzeichnis

AD oder ADS	Active Directory Services
AG	Auftraggeber
AZR	Ausländerzentralregister
B/B	Behörden und Bildungseinrichtungen (der Thüringer Polizei)
BHB	Betriebshandbuch
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BSI	Bundesamt für Sicherheit in der Informationstechnik
BV	Betriebsverantwortung
CMS	Content-Management-System
CN	Corporate Network
CMDB	Configuration Management Database
CSV	Comma-Seperated Values; Dateiformat
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
EAI	Enterprise Application Integration (Technologie um Schnittstellen und Dienste über einen unternehmensweiten Servicebus abzubilden)
EWO	Eigenname; Anwendung für Auskünfte von den Einwohnermeldeämtern
FLOSS	Free/Libre Open Source Software
GDI	Geodateninfrastruktur
GUI / NUI	Graphical User Interface / Natural User Interface
HP	Hewlett-Packard
IMP	Informationsmodell der Polizei, Quelle für aktuelles Release: BKA
INPOL	Informationssystem Polizei
IPSec	Internet Protocol Security
ISO	International Organization for Standardization

ISTPOL	Informationssystem der Thüringer Polizei
IT	Informationstechnik
KBA	Kraffahrt-Bundesamt
LDAP	Lightweight Directory Access Protocol
LZpD	Landeszentrale für polizeiliche Dienste
Mbit/s	Megabit pro Sekunde
MPLS	multi protocol label switching
MS	Microsoft
NTP	Network Time Protocol Server
NWR	Nationales Waffenregister
OAS	ORACLE-ApplicationServer
ORACLE-RAC	ORACLE RealApplicationCluster
PAG	Polizeiaufgabengesetz
PC	Personalcomputer
PDF	Portable Document Format; Dateiformat
PKI	Public-Key-Infrastructure
POG	Gesetz über die Organisation der Polizei des Landes Thüringen (Polizeiorganisationsgesetz)
R	Release
RADIUS	Remote Authentication Dial-In User Service
RM	RISC-Maschine (Prozessorarchitektur)
RZ	Rechenzentrum
SAGA	Standards und Architekturen für eGovernment Anwendungen
SCCM	System Center Configuration Manager
SDV	Stammdatenverwaltung
SIA	System Interface Agreement (Schnittstellenvereinbarung)

SLES	Suse Linux Enterprise Server
SM	Service Management (ITIL basierend)
SP	ServicePack
SQL	Structured Query Language; Datenbanksprache
SSO	Single Sign On
TH-Pol	Thüringer Polizei
ThürDSG	Thüringer Datenschutzgesetz
ThürPrüffristVO	Thüringer Prüffristenverordnung
TK	Telekommunikation
TLKA	Landeskriminalamt Thüringen
TSPA	Technologien, Standards, Protokolle, Architektur (eGovernment-Dokument des Freistaates Thüringen, Konzept)
UML	Unified Modelling Language
VM	Virtual Maschine
VPN	Virtual Private Network
WLS	WebLogic Server Management Pack Enterprise Edition
XML	Extensible Markup Language; Datenaustauschformat
ZBS	Zentrale Bußgeldstelle
TLRZ	Thüringer Landesrechenzentrum
ZFER	Zentrales Fahrerlaubnisregister
ZFZR	Zentrales Fahrzeugzulassungsregister
ZIMP	Zentrale Informationsmanagementplattform
ZKS	Zentraler Katalogserver
ZpIuK	Zentralstelle für polizeiliches Informations- und Kommunikationswesen

Dokumentenhistorie

Datum	Version	Bearbeiter	Inhalt
07.04.2011	1.0	[redacted]	[redacted]
15.06.2011	1.1	[redacted]	[redacted]
24.11.2011	1.2	[redacted]	[redacted]
06.12.2011	1.2	[redacted]	[redacted]
15.03.2012	1.3/1.4	[redacted]	[redacted]
20.03.2014	1.8	[redacted]	[redacted]
16.04.2015	2.0	[redacted]	[redacted]
19.02.2018	2.1	[redacted]	[redacted]
07.06.2018	2.1	[redacted]	[redacted]
18.06.2020	2.2	[redacted]	[redacted]
12.05.2022	2.3	[redacted]	[redacted]
04.11.2022 09.02.2023 21.08.2023 13.11.2023	2.4	[redacted]	[redacted]
19.12.2023	2.4	[redacted]	[redacted]

Schlagworte

Hier sind vom Verfasser des QM-Dokumentes die Schlagworte anzugeben, unter denen das Dokument recherchierbar sein soll.

☐	Arbeitssicherheit
☐	Arbeitszeit
☐	Asservate
☐	Ausbildung
☐	Ausstattung
☐	Beschaffung
☐	Besprechungen
☐	Datenauswertung
☐	Datenschutz
☐	Datensicherung
☐	Dienstbetrieb
☐	Dienstreise
☐	Dokumentation
☐	Einsatz
☐	Einsatz- & Ermittlungsunterstützung
☐	Ermittlungen
☐	Forensik
☐	Fortbildung
☐	Gebäudeleittechnik
☐	Geheimschutz
☐	Geschäftsgang
☐	Geschäftsordnung
☐	Gremien
☐	Innerdienstliche Regelungen
☒	IuK
☐	Kfz
☐	Kriminaltechnik
☐	Meldedienst/Nachrichtenaustausch
☐	Mess- und Prüfmittel
☐	Personal
☐	Prüfverfahren
☐	Reinigung
☐	Schriftgut
☐	Unfall
☐	Urlaub
☐	Wartung
☐	Zeichnungsverfahren
☐	
☐	
☐	
☐	
☐	

Freigabeprozess von QM-Dokumenten

Sachbearbeiter:	[redacted]
	Name elektr. gez
*Leiter Sachbereich **D71.1**:*	[redacted]
	Name elektr. gez
*Leiter Dezernat **D71**:*	[redacted]
	Name elektr. gez
*Leiter Abteilung **7** :*	[redacted]
	Name elektr. gez
*Mitzeichnung **DL72**:*	[redacted]
	Name elektr. gez
*Mitzeichnung **DL53**:*	[redacted]
	Name elektr. gez
*Mitzeichnung **AL5**:*	[redacted]
	Name elektr. gez
*Mitzeichnung **V/IT**:*	[redacted]
	Name elektr. gez
*Mitzeichnung **BAfIS** erforderlich:*	☒ Ja ☐ Nein
	elektr. gez
*Mitzeichnung **DSB** erforderlich:*	☒ Ja ☐ Nein
	elektr. gez
*Mitzeichnung **ÖPR** erforderlich:*	☐ Ja ☐ Nein
	elektr. gez
*Zustimmung **TMIK** erforderlich:*	☐ Ja ☒ Nein mit Erlass vom: Aktenzeichen:
*Mitzeichnung **L/LS**:*	[redacted]
	Name elektr. gez
Bestätigung/Schlusszeichnung:	[redacted]
	elektr. gez
Belehrung:	☐ Ja ☒ Nein Turnus:
Einarbeitung in die Liste gültiger Dokumente:	[redacted]
	erledigt: elektr. gez.