Staatliche Kunstsammlungen Dresden

Die Staatlichen Kunstsammlungen Dresden (SKD) suchen zum nächstmöglichen Zeitpunkt, in Vollzeit, einen/eine

**Chief Information Security Officer (CISO) (d/m/w)**

(bei Vorliegen der persönlichen Voraussetzungen in der **Entgeltgruppe 13 TV-L**)

zur strategischen Stärkung der Informationssicherheit und Modernisierung der IT-Landschaft der SKD. Die Stelle ist zunächst auf zwei Jahre befristet. Eine längerfristige Zusammenarbeit wird angestrebt. Die Vereinbarkeit von Beruf und Familie hat bei den Staatlichen Kunstsammlungen Dresden einen hohen Stellenwert. Soweit zwingende dienstliche Belange nicht entgegenstehen, ist der ausgeschriebene Arbeitsplatz – auch bei Wahrnehmung von Vorgesetzten- und Leitungsaufgaben – grundsätzlich teilzeitgeeignet.

Die Staatlichen Kunstsammlungen Dresden (SKD) bilden mit ihren zahlreichen Museen, Sammlungen und Archiven einen der bedeutendsten Museumsverbünde weltweit. Gemeinsam stehen die historisch gewachsenen Sammlungen für eine beeindruckende thematische Vielfalt. In prachtvollen historischen Bauten im Herzen Dresdens sowie an weiteren Orten in Sachsen und weit darüber hinaus machen die SKD ihre einzigartigen Bestände für die Öffentlichkeit erlebbar.

Die Wurzeln der Sammlungsvielfalt liegen in der Zeit der sächsischen Kurfürsten und Könige und gehen auf eine jahrhundertelange Tradition zurück. Jedes der Millionen von Objekten öffnet Fenster in globale Kunst- und Kulturwelten. Über die Bewahrung des ihr anvertrauten reichen Erbes hinaus beleben die SKD es durch inspirierende Ausstellungen und zukunftsweisende Vermittlungsformate unterstützt durch zahlreiche regionale, nationale und internationale Kooperationen.

Als wissenschaftlich arbeitende Institution steht die sammlungsübergreifende und objektbezogene Forschung im Zentrum. Mit disziplinenübergreifenden Projekten im Verbund setzen die SKD nicht zuletzt in der Provenienzforschung Maßstäbe. Rund 400 hochqualifizierte Mitarbeitende gestalten dieses dynamische Netzwerk und tragen mit ihrer Begeisterung und ihrem fundierten Wissen zur Vermittlung und Präsentation des reichen Erbes an Kunst und Kultur bei.

## Ihre Aufgaben

**Strategische Sicherheitsführung**

- Entwicklung und Verantwortung für die ganzheitliche Informationssicherheitsstrategie der SKD

- Aufbau und kontinuierliche Weiterentwicklung eines Information Security Management Systems (ISMS) orientiert an ISO 27001 und BSI-Grundschutz (Risikoanalysen, Richtlinien, Kontrollen)
- direkte Berichtslinie zur Hausleitung/Geschäftsführung, zentrale Ansprechperson für alle strategischen Sicherheitsfragen

**Aufbau und Leitung des CISO-Teams**

- Aufbau eines spezialisierten CISO-Teams mit klaren Rollen in den Bereichen Governance/Risikomanagement, technische Sicherheit/Härtung, Incident Response/Krisenmanagement, Identity- und Access-Management sowie Monitoring/Threat Detection
- Definition von Zuständigkeiten, Prozessen und Schnittstellen zur IT-Abteilung und zu externen Dienstleistern, klare Trennung von Betrieb und Security bei enger Zusammenarbeit

**Technische Sicherheitsverantwortung**

- Gesamtverantwortung für Vulnerability- und Patch-Management mit Fokus auf exponierte Systeme und „Crown Jewels" (AD, Hypervisor, Backups)
- Konzeption, Auswahl und Steuerung von MDR/SOC- und Security-Monitoring-Lösungen (Endpoints, Netzwerkkomponenten, AD-Logs, Virtualisierung, Backup)
- Vorgabe von Härtungs- und Konfigurationsstandards für Server, Clients, Netzwerk und sicherheitsrelevante Systeme

**Incident Response, Krisenmanagement und Compliance**

- Aufbau und Betrieb eines professionellen Incident-Response- und Krisenmanagement-Prozesses inkl. Runbooks, Notfallhandbuch, Übungen und spezifischer Ransomware-Playbooks
- Steuerung externer Dienstleister (IT-Dienstleister, Hoster, MDR-Provider) hinsichtlich Sicherheitsanforderungen, SLAs, Reporting und klarer Verantwortungsteilung
- enge Zusammenarbeit mit Datenschutz (DSGVO), Rechtsabteilung, Fachabteilungen und Behörden (z.B. Kulturministerium, ggf. BSI/LAND-CERT) zur Einhaltung aller regulatorischen Vorgaben

**Transformation zu moderner Cloud-Sicherheitsarchitektur**

- Entwicklung einer mittel- bis langfristigen Roadmap, die die bestehende On-Premises-Infrastruktur schrittweise in eine moderne, cloud-basierte Sicherheitsarchitektur überführt (Zero Trust, Cloud-Identity, sichere SaaS-Nutzung, Cloud-Backups)
- gezielter Aufbau von Cloud-Security-Kompetenzen im CISO-Team (z.B. Microsoft 365/Azure Security, Cloud IAM, Conditional Access, Defender/CASB), Absicherung hybrider Szenarien und schrittweise sichere Migration von Workloads in die Cloud

**Sicherheitskultur und Awareness**

- Etablierung einer nachhaltigen Sicherheitskultur durch Awareness-Programme, Schulungen und klare Richtlinien für Mitarbeitende, Führungskräfte und IT-Personal
- Verankerung von Informationssicherheit als selbstverständlichem Bestandteil des Arbeitsalltags in allen Museen und Verwaltungsbereichen

## Ihr Profil

**Formale Qualifikationen**

- abgeschlossenes Studium der Informatik, Wirtschaftsinformatik oder vergleichbare Qualifikationen

- wünschenswert: Zertifizierungen im Bereich Informationssicherheit (z.B. CISSP, CISM, CISA, ISO-27001-Lead-Implementer oder Vergleichbares)

**Berufserfahrung**

- mindestens 7 Jahre Berufserfahrung im Bereich Informationssicherheit, davon mindestens 3 Jahre in leitender Funktion
- idealerweise Erfahrung in einer öffentlichen Einrichtung, einem Kultur- oder Wissenschaftsbetrieb oder einer vergleichbaren kritischen Umgebung
- nachweisbare Praxis in der Abwehr oder Bewältigung komplexer Cyberangriffe, insbesondere Ransomware-Vorfälle
- Erfahrung im Aufbau und in der Führung von Security-Teams sowie Steuerung von externen Dienstleistern im Bereich von Informationssicherheit

**Technische Expertise – aktuelle Infrastruktur**

- tiefes Verständnis von Netzwerk- und DMZ-Design, Firewall-Konzepten, Mikrosegmentierung, VPN-Architekturen sowie der Verhinderung lateraler Bewegung
- fundierte Kenntnisse in Microsoft-Umgebungen (Active-Directory-Härtung, Windows-Server-Security, Privileged-Access-Management, Trennung von Admin- und Benutzerkonten)
- Erfahrung mit Virtualisierung (ESXi/vCenter-Security, Hypervisor-Härtung, sichere Verwaltung)
- ausgeprägte Kenntnisse in Backup- und Recovery-Konzepten (ransomwareresiliente Backups, Immutable/Offline-Backups, Wiederherstellungstests)
- Praxis im Betrieb von MDR/XDR, SIEM und Log-Management inkl. Korrelation von Endpoint-, Netzwerk-, AD-, Hypervisor- und Backup-Events
- Erfahrung im Vulnerability-Management

**Technische Vision – Cloud und moderne Architekturen**

- Erfahrung und klare Vorstellungen zu modernen, Identity-zentrierten und Zero-Trust-Architekturen
- Kenntnisse in Cloud-Security (Microsoft 365, Azure Security, idealerweise Grundlagen in AWS/GCP)
- Erfahrung mit Cloud Identity und Access Management (z.B. Entra ID, Conditional Access, MFA) sowie sicheren Hybrid-Szenarien und Cloud-Migration.
- idealerweise vertraut mit Themen wie Cloud Security Posture Management (CSPM), Cloud Access Security Broker (CASB) und DevSecOps-Ansätzen

**Persönliche Kompetenzen**

- Fähigkeit, komplexe technische Sachverhalte verständlich für Nicht-Techniker (Museumsleitung, Verwaltung, Gremien) aufzubereiten und belastbare Entscheidungsvorlagen zu erstellen
- hohe Eigenverantwortung, Durchsetzungsstärke und diplomatisches Geschick im Umgang mit unterschiedlichen Stakeholdern (Geschäftsführung, IT, Dienstleister, Behörden)
- strukturierte, analytische Arbeitsweise, ausgeprägtes Risikobewusstsein und pragmatische Priorisierung
- Krisenfestigkeit und nachgewiesene Erfahrung in der Steuerung von Security-Incidents unter Zeitdruck
- Erfahrung im Change-Management und in Transformationsprozessen bei laufendem Betrieb
- Fähigkeit zum Aufbau, zur Führung und zur Weiterentwicklung von Teams
- sehr gute Deutschkenntnisse in Wort und Schrift; Englischkenntnisse von Vorteil

## Wir bieten

- eine verantwortungsvolle Führungsposition mit direkter Berichtslinie zur Geschäftsführung in einer der bedeutendsten Kultureinrichtungen Deutschlands
- die Möglichkeit, nach einem einschneidenden Sicherheitsvorfall die Informationssicherheit der SKD von Grund auf neu aufzubauen und zu professionalisieren
- Budget und Mandat zum Aufbau eines eigenen CISO-Teams mit klaren Kompetenzen
- Gestaltungsspielraum für die Entwicklung einer modernen, zukunftssicheren Security-Architektur (On-Prem und Cloud)
- enge Zusammenarbeit mit Geschäftsführung, IT-Leitung, Fachabteilungen und externen Spezialisten
- Arbeitsvertrag nach Tarifvertrag für den öffentlichen Dienst der Länder (TV-L)
- 30 Tage Urlaub, dienstfreie Tage am 24.12. und 31.12. sowie Jahressonderzahlung
- flexible Arbeitszeitgestaltung und Möglichkeit des mobilen Arbeitens lt. Dienstvereinbarung
- betriebliche Altersvorsorge über die Versorgungsanstalt des Bundes und der Länder (VBL)
- Job-Ticket oder Zuschuss Deutschlandticket
- kostenfreier Besuch der SKD-Museen und Sammlungen für alle Mitarbeitenden
- zahlreiche attraktive museumsinterne Veranstaltungen + Sonderausstellungen
- ein breites Spektrum an Fort- und Weiterbildungsmöglichkeiten
- berufliche Weiterentwicklungsmöglichkeiten innerhalb der Abteilungen/Museen und im gesamten Verbund der SKD
- Angebote der Gesundheitsförderung
- sonstige Vergünstigungen bei lokalen Anbietern

## Kontakt

Wir freuen uns über Ihre Bewerbung, unabhängig von Geschlechtsidentität, Nationalität, ethnischer und sozialer Herkunft, Religion, Behinderung, Alter sowie sexueller Orientierung.

Mit Ihrer Bewerbung erteilen Sie Ihr Einverständnis zur Verarbeitung Ihrer persönlichen Daten bis zum Abschluss des Auswahlverfahrens. Vorstellungskosten können leider nicht übernommen bzw. erstattet werden. Nähere Auskünfte zum Aufgabengebiet erhalten Sie unter der Rufnummer 0351/49147546.

Bewerbungen richten Sie bitte bis zum **27.05.2026** an unser Online-Bewerberportal unter der Adresse https://jobs.skd.museum/.

Bitte beachten Sie, dass ausschließlich Bewerbungen über unser Online-Bewerbungsportal berücksichtigt werden, Bewerbungen per E-Mail, Post oder über andere Kommunikationswege werden nicht akzeptiert. Im Auswahlverfahren werden nur diejenigen Bewerbungen einbezogen, die zu den festgelegten Stichtagen vollständig eingegangen sind. Nach Ablauf der jeweiligen Fristen eingehende Bewerbungen werden nicht berücksichtigt.

Hier geht es direkt zur Stellenausschreibung
Hier geht es direkt zum Bewerbungsformular