Physical Security Policy

vStream Digital Media / ShineVR

Last updated 03/06/25

Definitions

Term	**Definition**
Company	means vStream Digital Media
ShineVR	means the ShineVR product developed and operated by vStream Digital Media
GDPR	means the General Data Protection Regulation
Responsible Person	means Andrés Pitt, CTO
Data Centre	Specialized building housing computer systems and associated components such as telecommunications and storage systems, including environmental controls and security devices
Physical Access Control	Security measures restricting physical entry to facilities, rooms, or equipment
Company Premises	vStream Digital Media office at 37 Leeson Close, Dublin 2, D02 H344, Ireland
Production Data	Live customer data, including ShineVR trial data and healthcare information
Biometric Authentication	Authentication based on unique physical characteristics (fingerprints, facial recognition, iris scans)

Term	Definition
Environmental Controls	Systems managing temperature, humidity, fire suppression, and power supply for IT infrastructure

1. POLICY STATEMENT

vStream Digital Media operates a **cloud-first infrastructure model** with **no customer or production data hosted at Company premises**. All customer data, ShineVR trial data, and production systems reside exclusively on Google Cloud Platform infrastructure in European data centres.

This Physical Security Policy establishes requirements for two distinct security environments:

1. **Data Centre Physical Security:** Complete reliance on Google Cloud Platform's comprehensive physical security controls for data centres housing production systems and customer data
2. **Company Office Physical Security:** Basic physical security measures for employee workspace at Company premises in Dublin, Ireland

The Company maintains no data centre facilities and does not manage physical security for production infrastructure. All data centre physical security is provided by Google Cloud Platform in their certified facilities in the Netherlands and Belgium.

2. PURPOSE

The purpose of this policy is to:

- Document reliance on Google Cloud Platform for data centre physical security
- Establish physical security requirements for Company office premises
- Protect Company-owned equipment and assets
- Define physical access controls for office facilities
- Establish equipment disposal and decommissioning procedures
- Ensure compliance with GDPR, ISO 27001, and customer security requirements
- Define roles and responsibilities for physical security
- Support business continuity through appropriate physical security measures
- Provide evidence of physical security controls for audit and compliance purposes

3. SCOPE

This policy applies to:

3.1 Data Centre Facilities (Google Cloud Platform)

- Google Cloud data centres in europe-west4-a (Eemshaven, Netherlands)
- Google Cloud data centres in europe-west1-b (St. Ghislain, Belgium)
- All infrastructure hosting production systems, customer data, and ShineVR applications
- Physical security for these facilities is **managed entirely by Google Cloud Platform**

3.2 Company Office Premises

- Company office at 37 Leeson Close, Dublin 2, D02 H344, Ireland
- Employee workspaces and meeting rooms
- Company-owned equipment and devices
- Physical asset storage and disposal

3.3 Personnel

- All employees, contractors, and temporary staff of vStream Digital Media
- Visitors to Company premises
- Third-party personnel with physical access to Company facilities

Important Context: The Company operates from a small office with controlled access. No customer data, production data, or ShineVR trial data is stored at Company premises. All production systems are cloud-hosted.

4. DATA CENTRE PHYSICAL SECURITY (GOOGLE CLOUD PLATFORM)

4.1 Cloud-First Model

Complete Reliance on Google Cloud Platform:

- vStream does **not manage, operate, or maintain** physical data centre facilities
- All customer data and production systems hosted on Google Cloud Platform infrastructure
- Google Cloud provides comprehensive physical security for their data centres
- Data centres located in:
  - **europe-west4-a** (Eemshaven, Netherlands) - Primary
  - **europe-west1-b** (St. Ghislain, Belgium) - Secondary
- EU data residency maintained (no data stored outside Europe)

Company's Role:

- Select secure cloud provider with appropriate certifications
- Review and verify Google Cloud's security certifications and compliance
- Document reliance on Google Cloud physical security controls

- Monitor Google Cloud security notifications and updates
- Participate in Google Cloud security programmes
- Maintain evidence of Google Cloud compliance for audits

4.2 Google Cloud Data Centre Physical Security Controls

Documented for Compliance and Audit Purposes:

The following physical security controls are documented by Google Cloud Platform as implemented at their data centres. **This information is derived from Google Cloud's official security documentation and should be verified against current Google Cloud security whitepapers and compliance reports.**

Sources:

- Google Cloud Infrastructure Security Design Overview (https://cloud.google.com/security/infrastructure/design)
- Google Cloud Security Whitepaper (https://cloud.google.com/security/overview/whitepaper)
- Google Cloud Compliance Resource Centre (https://cloud.google.com/security/compliance)
- Google Cloud SOC 2 Reports (available to customers via Compliance Reports Manager)
- Google Cloud ISO 27001 Certification documentation

Physical Security Controls as Documented by Google Cloud:

Perimeter Security:

According to Google Cloud's Infrastructure Security Design Overview, Google data centres feature multiple layers of physical security including controlled perimeters, physical barriers, and access control systems. Specific measures include:

- Data centres located in nondescript buildings
- Physical barriers and controlled entry points
- 24/7 perimeter monitoring
- Vehicle access controls and inspection
- Separate delivery and visitor entrances

Access Control:

Google Cloud documentation describes comprehensive access control measures:

- Multi-factor authentication for facility access
- Biometric authentication systems
- Security badges with photo identification

- Escort requirements for visitors
- Access granted on need-to-enter basis only
- Regular access review and revocation for terminated personnel

Surveillance and Monitoring:

As documented in Google Cloud's security whitepapers:

- 24/7 video surveillance of data centre areas
- Security operations centre monitoring
- Intrusion detection systems
- Alarm systems for unauthorized access attempts
- Video footage retained for security investigations

Physical Security Personnel:

Google Cloud maintains professional security staff:

- Trained security guards on-site 24/7
- Security guard screening and background checks
- Regular security patrols
- Incident response procedures
- Coordination with local law enforcement

Environmental Controls:

Google Cloud's Infrastructure Security Design Overview documents environmental protection measures:

- Redundant power supplies with backup generators
- Uninterruptible Power Supply (UPS) systems
- Climate control systems (cooling and humidity management)
- Fire detection and suppression systems
- Water leak detection
- Natural disaster protection measures (earthquake-resistant design where applicable)

Hardware Security and Decommissioning:

Google Cloud's security documentation describes hardware lifecycle security:

- Server racks locked and access-controlled
- Asset tracking and inventory management
- Secure hardware decommissioning procedures:
    - Multi-step data sanitization process

    - Cryptographic erasure (encryption key destruction)
    - Degaussing for magnetic media
    - Physical destruction of storage media
    - Documented chain of custody
- No customer access to physical servers

Important Note: Customers should refer to current Google Cloud security documentation for the most up-to-date information on physical security controls. Google Cloud regularly updates their security documentation and certifications. The Company reviews Google Cloud security documentation annually and maintains copies of relevant compliance reports for audit purposes.

4.3 Google Cloud Security Certifications

Google Cloud maintains comprehensive security certifications:

- **ISO/IEC 27001:** Information Security Management
- **ISO/IEC 27017:** Cloud Security
- **ISO/IEC 27018:** Cloud Privacy
- **SOC 2 Type II:** Service Organization Controls
- **SOC 3:** Security, Availability, and Confidentiality
- **PCI DSS:** Payment Card Industry Data Security Standard
- **HIPAA:** Health Insurance Portability and Accountability Act
- Various national and regional certifications

Company's Verification Process:

- Annual review of Google Cloud compliance documentation
- Verification of current certification status
- Review of Google Cloud security updates and bulletins
- Participation in Google Cloud security webinars and training
- Documentation of Google Cloud certifications for customer audits

4.4 Company Responsibilities for Cloud Physical Security

What vStream Does:

- Select and contract with certified cloud provider (Google Cloud Platform)
- Define data residency requirements (EU only)
- Review Google Cloud security certifications annually
- Monitor Google Cloud security notifications
- Maintain documentation of Google Cloud security controls for audits
- Provide customers with evidence of data centre security (via Google Cloud documentation)

What vStream Does Not Do:

- Manage or operate data centre physical security
- Conduct physical security audits of Google Cloud data centres (rely on third-party certifications)
- Maintain physical access to data centre facilities
- Dispose of data centre hardware (managed by Google Cloud)
- Implement physical environmental controls (managed by Google Cloud)

5. COMPANY OFFICE PHYSICAL SECURITY

5.1 Office Context and Risk Profile

Office Environment:

- Small office with controlled building access
- Limited employee count (all personnel known)
- Shared office building with building security
- **No customer data or production data stored on premises**
- **No servers or production infrastructure at office**
- Office used primarily for:
    - Employee workspace
    - Meetings and collaboration
    - Development on laptops (accessing cloud resources)

Security Risk Assessment:

- **Low risk to customer data** (no customer data at premises)
- **Medium risk to Company assets** (laptops, equipment)
- **Low risk to business continuity** (cloud-based systems enable remote work)
- Physical security important for employee safety and asset protection

5.2 Building Access Control

Building Security:

- Office located in multi-tenant building
- Building access controlled by landlord/building management
- Building security includes:
    - Reception desk during business hours
    - Access card system for after-hours entry
    - CCTV in common areas (building-managed)

Company Office Access:

- Office door locked when unattended
- Keys issued to permanent employees only
- Key return upon employee termination
- Visitors must be escorted by employee
- Visitor log maintained (name, company, purpose, time in/out, employee host)

After-Hours Access:

- Building access card required for after-hours entry
- Employees notified of building access card procedures
- Lost or stolen access cards reported immediately to building management and CTO
- Access cards deactivated upon employee termination

5.3 Visitor Management

Visitor Procedures:

- All visitors must be pre-arranged with employee host
- Visitors check in with employee host (not unattended in reception)
- Visitor log maintained including:
    - Visitor name and company
    - Purpose of visit
    - Date and time in/time out
    - Employee host name
- Visitors escorted at all times while in office
- No visitor access to employee workstations or Company systems
- Visitors use segregated guest wireless network (if implemented)
- Confidential information secured before visitor meetings

Visitor Restrictions:

- Visitors not permitted in areas where confidential information displayed
- No photography in office without approval
- Visitors do not access Company computers or systems
- Visitor access documented in visitor log

5.4 Clear Desk and Clear Screen Policy

Clear Desk Requirements:

- Sensitive documents secured in locked drawers when not in use
- Confidential printouts not left unattended on printers
- Whiteboards with confidential information erased after meetings
- Secure disposal of confidential documents (shredding)
- No customer data printed (all data accessed via cloud with encryption)

Clear Screen Requirements:

- Computers automatically lock after 5 minutes of inactivity
- Employees lock screens when leaving desk (Windows + L, Command + Control + Q)
- Password-protected screensavers enabled
- Monitors positioned to prevent unauthorized viewing from windows or common areas

5.5 Equipment and Asset Security

Company-Owned Equipment:

- IT hardware asset register maintained (see Asset Management)
- Asset register includes:
    - Asset type and model
    - Serial number
    - Assignment to employee
    - Location
    - Acquisition date
    - Status (active, storage, disposed)
- Asset tags applied to Company-owned equipment where practical

Laptop and Device Security:

- Laptops locked to desks with cable locks (if working in office)
- Laptops secured in locked drawers or taken home (not left in office overnight)
- Company devices encrypted (see Encryption Policy and BYOD Policy)
- Lost or stolen devices reported immediately to CTO
- Remote wipe capability enabled on Company devices (via Google Workspace)

Peripheral Security:

- External hard drives and USB drives encrypted
- Removable media not used for Company data (all data in cloud)
- Unused equipment stored in locked cabinets
- Equipment surplus securely stored until disposal

5.6 Office Environmental Controls

Basic Environmental Protection:

- Fire extinguishers present and inspected (building-managed)
- Smoke detectors installed (building-managed)
- Emergency exit routes clearly marked
- Emergency evacuation procedures displayed

- First aid kit available
- No specialized environmental controls required (no servers at premises)

Building Systems:

- HVAC (heating, ventilation, air conditioning) managed by building
- Electrical systems managed by building
- Water leak detection in building
- Building maintenance schedules communicated to tenants

Employee Responsibilities:

- Report environmental hazards to building management
- Follow emergency evacuation procedures
- Do not prop open fire doors
- Report malfunctioning smoke detectors or fire extinguishers

6. HARDWARE DISPOSAL AND DECOMMISSIONING

6.1 Company-Owned Device Disposal

Disposal Process for Company Devices:

1. **Employee Termination or Device Replacement:**

    - Device returned to CTO or designated IT personnel
    - Device wiped using secure data erasure methods
    - For Google Workspace devices: factory reset and Google account removal
    - Data backed up to Google Drive before wiping (if required)
    - Google account data reassigned to employee's manager

2. **Data Erasure:**

    - Full disk encryption keys destroyed (rendering data unrecoverable)
    - Operating system reinstall or factory reset
    - Multiple-pass data overwrite (if encryption keys cannot be destroyed)
    - Verification of successful data erasure
    - Documentation of data erasure in disposal log

3. **Physical Disposal:**

    - Wiped devices donated to charity, sold, or recycled
    - If device cannot be wiped: physical destruction of storage media
    - Certificate of disposal obtained from disposal vendor (if applicable)

    - Asset register updated with disposal date and method

Disposal Documentation:

- Asset identification (serial number, asset tag)
- Data erasure method and verification
- Disposal method (donation, recycling, destruction)
- Disposal date
- Person responsible for disposal
- Certificate of disposal (if applicable)

6.2 Data Centre Hardware Disposal (Google Cloud)

Google Cloud Hardware Decommissioning:

- vStream does **not physically dispose** of data centre hardware
- All production infrastructure hosted on Google Cloud Platform
- Google Cloud manages hardware lifecycle including decommissioning
- Google Cloud decommissioning process includes:
    - Multi-step data sanitization
    - Cryptographic erasure (encryption key destruction)
    - Degaussing for magnetic media
    - Physical destruction of storage media (shredding, crushing)
    - Chain of custody documentation
    - Zero-touch decommissioning (no customer interaction)

Company Documentation:

- Document reliance on Google Cloud decommissioning procedures
- Provide customers with Google Cloud disposal certifications upon request
- No disposal records kept by vStream (managed by Google Cloud)

6.3 Removable Media Disposal

USB Drives, External Hard Drives, Backup Media:

- Company does not use removable media for production data (all data in cloud)
- If removable media used:
    - Encrypt all data on removable media
    - Wipe removable media before disposal using secure erasure tools
    - Physically destroy removable media containing sensitive information
    - Document disposal in disposal log

Backup Media Disposal:

- All backups stored in Google Cloud Storage (no physical backup media)
- Google Cloud manages backup storage lifecycle
- See Backup and Recovery Policy for backup retention and deletion procedures

7. MOBILE DEVICE MANAGEMENT

7.1 Company Device Security

Company-Issued Mobile Devices:

- Company does not currently issue mobile phones to employees
- If Company-issued mobile devices used in future:
    - Device encryption mandatory
    - Screen lock with PIN/biometric authentication required
    - Remote wipe capability enabled
    - Lost or stolen device reporting procedures
    - Device tracking enabled (Find My Device, Find My iPhone)

7.2 Personal Device Security (BYOD)

Bring Your Own Device Policy:

- Employees use personal devices for work (primarily mobile phones)
- BYOD Policy establishes security requirements for personal devices
- Key BYOD requirements:
    - Device encryption enabled
    - Screen lock with strong passcode/biometric
    - Anti-malware software installed
    - Operating system kept updated
    - Separation of work and personal data (via Google Workspace)
- See BYOD Policy for comprehensive requirements

8. PHYSICAL SECURITY INCIDENTS

8.1 Incident Types

Physical Security Incidents:

- Lost or stolen Company device
- Unauthorized physical access to office
- Theft of Company property
- Physical damage to equipment
- Security violation (propped door, lost keys, etc.)
- Visitor policy violation

- Environmental incident (fire, flood, power outage)

8.2 Incident Reporting

Reporting Procedures:

- All physical security incidents reported immediately to CTO
- Lost or stolen devices reported within 1 hour of discovery
- After-hours incidents: Call CTO directly at (086) 788 6570
- Document incident details:
    - What happened
    - When and where
    - Who was involved
    - What data or systems potentially affected
    - Immediate actions taken

8.3 Incident Response

Lost or Stolen Device Response:

1. Employee reports to CTO immediately
2. CTO initiates remote wipe via Google Workspace (if Company device)
3. Account passwords changed (if account credentials on device)
4. Monitoring for unauthorized access to Company systems
5. Police report filed (if appropriate)
6. Insurance claim filed (if applicable)
7. Incident documented in incident register
8. Post-incident review to prevent recurrence

Physical Breach Response:

1. Ensure physical safety of personnel
2. Contact building security and/or police (if ongoing threat)
3. Assess what was accessed or taken
4. Check for unauthorized system access (review access logs)
5. Secure affected area
6. Document incident
7. Remediate vulnerabilities
8. Post-incident review

See Incident Management Policy for comprehensive incident response procedures.

9. BUSINESS CONTINUITY AND DISASTER RECOVERY

9.1 Physical Disaster Impact

Office Disaster Scenarios:

- Fire, flood, or other physical damage to office
- Extended power outage
- Building access denial
- Equipment theft or destruction

Impact Assessment:

- **Customer data impact:** None (no customer data at office)
- **Production systems impact:** None (cloud-hosted on Google Cloud)
- **Business operations impact:** Minimal (remote work capable)
- **Employee safety:** Primary concern in disaster scenarios

9.2 Business Continuity Measures

Remote Work Capability:

- All employees equipped with laptops for remote work
- All Company data stored in Google Drive (cloud-based)
- Production systems accessed via cloud (Google Cloud Platform)
- Communication via Google Workspace (Gmail, Meet, Chat)
- No dependency on physical office for business operations

Recovery Procedures:

- In event of office unavailability:
    - Employees work remotely from home
    - Meetings conducted via Google Meet
    - No impact to production systems or customer data
    - Temporary workspace sourced if extended office loss
- Recovery Time Objective (RTO): Immediate (remote work)
- Recovery Point Objective (RPO): Zero (all data in cloud)

See Backup and Recovery Policy for comprehensive DR procedures.

9.3 Google Cloud Data Centre Disaster

Data Centre Incident Scenarios:

- Google Cloud data centre physical damage

- Regional outage
- Natural disaster affecting data centre

Google Cloud Resilience:

- Multi-region architecture (Netherlands and Belgium)
- Automatic failover between regions
- Google Cloud's disaster recovery capabilities
- Google Cloud SLAs for availability
- Company does not manage data centre disaster recovery (reliance on Google Cloud)

Company Response to Data Centre Incident:

- Monitor Google Cloud Status Dashboard
- Activate incident response procedures if customer-facing service affected
- Communicate with customers per contractual obligations
- Document incident and Google Cloud response
- Post-incident review and lessons learned

10. ASSET MANAGEMENT

10.1 IT Hardware Asset Register

Asset Register Contents:

- **Asset identification:**
  - Asset type (laptop, monitor, phone, etc.)
  - Make and model
  - Serial number
  - Asset tag (if applicable)
- **Asset assignment:**
  - Assigned employee name
  - Assignment date
  - Location (office, remote, storage)
- **Asset lifecycle:**
  - Acquisition date and cost
  - Warranty information
  - Disposal date and method
  - Current status (active, storage, disposed)

Asset Register Maintenance:

- Asset register updated within 5 working days of changes
- New equipment added to register upon acquisition

- Asset transfers documented (employee to employee)
- Disposed equipment marked in register with disposal details
- Annual comprehensive asset inventory audit

10.2 Software Asset Management

Software Inventory:

- Software licenses tracked separately from hardware assets
- Google Workspace licenses assigned per user
- Development tools and software licenses documented
- Cloud service subscriptions tracked
- Regular review of software licenses for cost optimization

10.3 Asset Audits

Annual Asset Audit:

- Physical verification of all Company-owned assets
- Reconciliation with asset register
- Identification of missing or unaccounted assets
- Investigation of discrepancies
- Asset register corrections
- Disposal recommendations for obsolete equipment

11. TRAINING AND AWARENESS

11.1 Physical Security Training

Required Training:

- All new employees: Physical security awareness during induction
    - Office access procedures
    - Visitor management
    - Clear desk/clear screen policies
    - Device security
    - Lost/stolen device reporting
    - Emergency procedures
- Annual refresher training for all staff

Training Content:

- Physical security policy overview
- Office access and key management
- Visitor procedures and visitor log

- Equipment security and asset management
- Data disposal and device decommissioning
- Incident reporting procedures
- Social engineering awareness (tailgating, impersonation)

11.2 Emergency Procedures Training

Emergency Preparedness:

- Fire evacuation procedures
- Assembly point location
- Emergency contact numbers
- First aid responders
- Building-specific emergency procedures
- Annual emergency drill (building-managed)

12. COMPLIANCE AND REGULATORY REQUIREMENTS

12.1 GDPR Physical Security

GDPR Article 32 - Security of Processing:

- Physical security measures appropriate to risk
- Protection against accidental loss or destruction
- Physical access controls for processing facilities
- Documentation of physical security measures

GDPR Compliance:

- No personal data stored at Company premises (all data in cloud)
- Google Cloud provides appropriate physical security for personal data
- Device encryption protects personal data on employee devices
- Secure disposal ensures personal data irrecoverable
- Physical security incidents reported per breach notification requirements (if applicable)

12.2 ISO 27001 Physical Security Controls

ISO 27001 Annex A.11 - Physical and Environmental Security:

- A.11.1 Secure areas (office access control, visitor management)
- A.11.2 Equipment security (asset management, secure disposal)
- Compliance monitored via Google Cloud Security Command Centre (for data centres)
- Office security documented and auditable

12.3 Customer Security Requirements

Healthcare Customer Requirements:

- Physical security controls meet healthcare customer requirements
- Google Cloud physical security certifications available for customer audits
- Documentation of data centre physical security provided upon request
- No customer data at Company premises (reduces physical security risk)

13. ROLES AND RESPONSIBILITIES

Role	**Responsibilities**
CTO (Responsible Person)	Overall physical security policy ownership; Google Cloud physical security verification; office security oversight; asset register management; physical security incident response; policy review and updates; approval of equipment disposal
All Employees	Comply with office access procedures; follow clear desk/clear screen policy; secure Company equipment; report lost/stolen devices; escort visitors; report physical security incidents; participate in emergency drills; follow asset management procedures
Building Management	Building access control; CCTV in common areas; emergency systems; environmental controls (HVAC, fire suppression); building security patrols

14. POLICY REVIEW AND MAINTENANCE

Review Schedule:

- Annual policy review by CTO
- Review triggered by:
  - Significant physical security incidents
  - Changes to office location
  - Changes to Google Cloud provider or data centre locations
  - New regulatory requirements
  - Customer security requirement changes
  - Results of asset audits or security assessments

Policy Updates:

- All updates require CTO approval
- Changes communicated to all staff within 10 working days
- Updated policy published to Company policy repository
- Policy version history maintained

15. EXCEPTIONS

15.1 Exception Process

Requesting Physical Security Exceptions:

- Exceptions requested in writing to CTO
- Business justification required
- Risk assessment documented
- Compensating controls identified
- Time-limited exceptions preferred
- Permanent exceptions require CEO approval

Example Exceptions:

- After-hours office access without building security
- Equipment stored outside office (employee home office)
- Visitor access to restricted areas (with escort and business justification)

15.2 Work from Home Exceptions

Remote Work Physical Security:

- Employees working from home follow BYOD Policy requirements
- Home office physical security (locking doors, securing equipment)
- Home network security requirements (see Network Security Policy, BYOD Policy)
- No customer or production data stored locally on home devices

16. RELATED POLICIES AND DOCUMENTS

This policy should be read in conjunction with:

- Information Security Policy
- Cloud Security Policy
- Network Security Policy
- Encryption Policy
- BYOD Policy

- Access Management Policy
- Incident Management Policy
- Backup and Recovery Policy
- Media Retention and Disposal Policy
- Change Control Policy

17. CONTACT INFORMATION

Data Protection Officer / Chief Technology Officer:

Andrés Pitt
Email: andres@vstream.ie
Phone: (086) 788 6570
Available 24/7 for P1 physical security incidents (lost/stolen devices, security breaches)

Company Address:

vStream Digital Media
37 Leeson Close
Dublin 2, D02 H344
Ireland

Website: vstream.ie

APPENDIX A: GOOGLE CLOUD PHYSICAL SECURITY DOCUMENTATION

For Audit and Compliance Purposes:

The following official documentation is available from Google Cloud Platform regarding their data centre physical security and should be referenced for audit and compliance evidence:

Publicly Available Documentation:

1. **Google Cloud Infrastructure Security Design Overview**

    - URL: https://cloud.google.com/security/infrastructure/design
    - Contains: Comprehensive overview of Google's infrastructure security including physical security layers
    - Access: Publicly available, no login required

2. **Google Cloud Security Whitepaper**

- URL: https://cloud.google.com/security/overview/whitepaper
- Contains: Detailed security practices including data centre physical security
- Access: Publicly available, downloadable PDF

3. **Google Cloud Compliance Resource Centre**

- URL: https://cloud.google.com/security/compliance
- Contains: Certifications, compliance reports, and security documentation
- Access: Publicly available

4. **Google Cloud Trust Centre**

- URL: https://cloud.google.com/security
- Contains: Security overview, best practices, and compliance information
- Access: Publicly available

Customer-Only Documentation:

5. **SOC 2 Type II Reports**

- Access: Via Google Cloud Compliance Reports Manager (requires Google Cloud customer account)
- Contains: Detailed audit reports including physical security controls
- Location: Google Cloud Console > Compliance Reports Manager
- Frequency: Updated annually

6. **ISO 27001 Certificates**

- Access: Via Google Cloud Compliance Reports Manager
- Contains: ISO 27001 certification for Google Cloud services
- Location: Google Cloud Console > Compliance Reports Manager

7. **ISO 27017 (Cloud Security) Certificates**

- Access: Via Google Cloud Compliance Reports Manager
- Contains: Cloud-specific security certification
- Location: Google Cloud Console > Compliance Reports Manager

8. **ISO 27018 (Cloud Privacy) Certificates**

- Access: Via Google Cloud Compliance Reports Manager
- Contains: Cloud privacy certification
- Location: Google Cloud Console > Compliance Reports Manager

How to Access Customer-Only Documentation:

Via Google Cloud Console:

1. Log in to Google Cloud Console (console.cloud.google.com)
2. Navigate to: Security > Compliance Reports Manager
3. View and download available compliance reports and certifications
4. Reports available: SOC 2, ISO certifications, PCI DSS attestations

Via Google Cloud Support:

- Open support ticket requesting specific compliance documentation
- Compliance team can provide additional documentation for customer audits
- Support ticket system: cloud.google.com/support

Company Responsibilities:

Annual Review:

- CTO reviews Google Cloud security documentation annually (minimum)
- Verification of current certification status
- Documentation of review in compliance records
- Updated copies maintained for audit purposes

Audit Support:

- Compliance reports downloaded and maintained for customer audits
- Links to public Google Cloud documentation provided to auditors
- SOC 2 reports shared with customers under NDA (if required)
- ISO certificates provided to demonstrate compliance

Monitoring:

- Subscribe to Google Cloud security bulletins and updates
- Monitor Google Cloud Status Dashboard for security incidents
- Review Google Cloud security blog for updates
- Participate in Google Cloud security webinars and training

Documentation for Customer Audits:

When customers request evidence of physical security controls, provide:

1. Link to Google Cloud Infrastructure Security Design Overview (public)
2. Link to Google Cloud Security Whitepaper (public)
3. Current ISO 27001 certificate (from Compliance Reports Manager)

4. Current SOC 2 Type II report (under NDA if required)
5. Google Cloud Compliance Resource Centre link for customer verification

Documentation Update Schedule:

- Google Cloud updates security documentation regularly
- Major updates typically announced via Google Cloud blog
- Certifications renewed annually (ISO, SOC 2)
- Company reviews documentation annually (February each year)
- Ad-hoc review when customer audits require current documentation

Contact Information for Google Cloud Security Documentation:

For Public Documentation:

- Website: https://cloud.google.com/security
- Compliance: https://cloud.google.com/security/compliance

For Customer-Specific Documentation:

- Google Cloud Support: Open ticket via Cloud Console
- Compliance Reports Manager: Available in Google Cloud Console
- Email: compliance@google.com (for compliance-specific inquiries)

For Emergency Security Issues:

- Google Cloud Support (24/7)
- Report vulnerability: https://cloud.google.com/security/vulnerability-reporting