SFTP Policy Checklist for B2B Use Cases

Healthcare Data Exchange (PHI)

- Use AES-256 encryption for data in transit and at rest.

- Implement role-based access control (RBAC) and MFA.

- Maintain HIPAA-compliant audit logs and retention policies.

- Validate endpoints and use host key verification.

- Ensure Business Associate Agreements (BAAs) are in place.

Cross-Border Personal Data Transfers

- Enforce data residency controls and geo-fencing.

- Use GDPR-compliant encryption and access policies.

- Document data transfer impact assessments (DTIAs).

- Implement logging and breach notification workflows.

Vendor File Sharing (Insurance, Labs)

- Use temporary credentials or token-based access.

- Automate file delivery confirmations and alerts.

- Apply least privilege access and periodic reviews.

- Monitor for anomalous activity and failed transfers.

Financial Reporting & Audit Transfers

- Ensure non-repudiation via digital signatures or hash validation.

- Maintain immutable audit trails with timestamping.

- Use redundant SFTP paths for high availability.

- Align with SOX and SOC 2 audit requirements.

Employee Data Transfers (HR, Payroll)

- Encrypt sensitive personal data (PII/PHI).

- Use access logging and data masking where applicable.
- Implement automated breach detection and alerts.
- Align with GDPR and internal HR policies.

Legal Document Exchange

- Use chain-of-custody tracking and access revocation.
- Encrypt documents with strong cryptographic standards.
- Apply retention policies based on case type.
- Ensure secure authentication and endpoint validation.

Regulatory Submissions

- Automate delivery confirmations and SLA tracking.
- Use redundant transmission paths and failover systems.
- Maintain compliance logs and traceability reports.
- Align with DORA, SEC, or other regulatory mandates.

Universal Best Practices for SFTP

- Use SSH key-based authentication with rotation policies.
- Disable unused services and ports on SFTP servers.
- Monitor and alert on failed login attempts and unusual activity.
- Patch and update SFTP software regularly.
- Conduct regular penetration testing and vulnerability scans.
- Document SLAs and compliance mappings per use case.