Zayo Security Policy

Table of contents

Change History 2
1. Purpose, scope and Users 5
2. Compliance and exceptions 5
3. Management responsibilities 6
4. Legal, statutory, regulatory, and contractual requirements 6
5. Policy requirements 6
    5.1. Security Governance 6
    5.2. Audit 6
    5.3. Risk assessment 7
    5.4. Data classification 7
    5.5. Information retention and disposal 7
    5.6. Acceptable use of assets 8
        5.6.1. Prohibited activities 8
        5.6.2. Authorizations for asset use 8
        5.6.3. Taking assets off-site 8
        5.6.4. Internet use 8
        5.6.5. E-mail and other message exchange methods 10
        5.6.6. Use of Zoom 11
        5.6.7. Use of Artificial Intelligence (AI) 11
            5.6.7.1. Additional considerations 12
        5.6.8. Intellectual property and copyright 12
        5.6.9. Mobile devices 13
            5.6.9.1. Remote access 14
            5.6.9.2. Bring Your Own Device (BYOD) 15
    5.7. Handling of assets 15
        5.7.1. Information transfer 16
        5.7.2. Media handling 16
            5.7.2.1. Management of removable media 16
            5.7.2.2. Physical media in transit 16
            5.7.2.3. Media sanitization and disposal 17
        5.7.3. Return of assets 17
    5.8. User passwords 17
        5.8.1. Application service account passwords 18

5.9. Network security 19
5.10. Physical access control 19
5.11. Endpoint protection 19
5.11.1. Endpoint encryption 20
5.12. Incident response 20
5.13. Vulnerability and patch management 20
5.14. Log retention and management 21
5.15. Change management 21
6. Security awareness training 21
6.1. External User training 22
6.1.1. Vendors providing services onsite 22
6.1.2. Contributing contractors to Zayo deliverables 22
6.1.3. Contractors supporting Zayo 22
7. Release of Information 22
8. Control objectives 23
9. Roles and responsibilities 26
10. Definitions 29
11. Enforcement 32
12. Related documents 32
13. Validity and policy management 33