

Title: Modern Hire Information Security Policy	
Department: Information Security	Contact: Jamie Macko
Approval Date: 11/2022	Last Review Date: 11/2022 Review Period: Annual
Applicability: All employees, contractors, and vendors of Modern Hire and its affiliated entities who access or use Modern Hire technology or who process or store Modern Hire data, irrespective of location.	
Authority: The Executive Leadership Team subordinates and supports the policies defined within the Corporate Information Security Policy. It is enforceable as an extension of the Corporate Information Security Policy, under the direction of Modern Hire’s Board of Directors.	

Table of Contents

- 1. POLICY 4
- 2. SCOPE 4
- 3. Objective 4
- 4. RISK MANAGEMENT 5
 - 4.1. Risk Management..... 5
 - 4.2. Vendor Risk Management 6
 - 4.2.1. Due Diligence 6
 - 4.2.2. Vendor Risk Analysis 6
 - 4.2.3. Contract Execution 6
 - 4.2.4. Other Information Security requirements 7
- 5. INFORMATION SECURITY DEFINITIONS..... 7
- 6. Monitoring and Measuring the ISMS..... 8
- 7. INFORMATION SECURITY RESPONSIBILITIES 10
 - 7.1. Information Security Department..... 10
 - 7.2. Information Owner 11
 - 7.3. Custodian..... 11
 - 7.4. User Management..... 12
 - 7.5. User and Information Security Awareness Training..... 12
- 8. INFORMATION CLASSIFICATION 13
 - 8.1. Personally Identifiable Information (PII) 13
 - 8.2. Confidential Information 13
 - 8.3. Internal Information..... 14
 - 8.4. Public Information..... 14
- 9. COMPUTER AND INFORMATION CONTROL..... 14

9.1. Information Systems	14
9.2. Systems, Equipment, and Networks Must Be Secured	14
9.3. Ownership of Software	16
9.4. Installed Software	16
9.5. Patching	16
9.6. System and Application Monitoring	16
9.7. Modern Hire Operating Systems Hardening	17
9.8. Virus and Malware Protection.....	17
9.9. Encryption and Cryptographic Controls	17
9.10. Access Controls	17
9.10.1. Requests.....	18
9.10.2. Grants	18
9.10.3. Removals.....	18
9.10.4. Authorization.....	18
9.10.5. Identification/Authentication and Passwords.....	18
9.11. Modern Hire Password Policy.....	19
9.11.1. Minimum requirements	20
9.11.2. Password Access Standards	20
9.11.3. Administrator Account Standards	20
9.11.4. Local Administrator on Amazon AWS instance exception.....	21
9.12. Data Integrity	21
9.13. Information Owners.....	21
9.14. Data Processing Separation	22
9.15. Transmission Security.....	22
9.16. Remote Access.....	22
9.17. Network, Wireless Network and Network services.....	22
9.18. Physical Access and Security.....	22
9.19. Emergency Access.....	23
9.20. Equipment and Media Controls.....	23
9.20.1. Information Disposal / Media Re-Use of:	23
9.20.2. Accountability.....	24
9.20.3. Data backup and Storage	24
9.21. Removable Media.....	24
9.22. Data Transfer/Printing:.....	24

9.22.1. Electronic Mass Data Transfers	24
9.22.2. Other Electronic Data Transfers and Printing	24
9.23. Oral and Written Communications	25
9.24. Audit Controls and Logging.....	25
9.25. Evaluation – Penetration and Vulnerability Testing	25
9.26. Contingency Plan.....	26
9.26.1. Data Backup Plan	26
9.26.2. Disaster Recovery Plan	26
9.26.3. Emergency Mode Operation Plan	26
9.26.4. Testing and Revision Procedures	26
9.26.5. Applications and Data Criticality Analysis	27
9.27. Bring Your Own Device (BYOD).....	27
9.27.1. Acceptable Use.....	27
9.27.2. Devices and Support.....	28
9.27.3. Reimbursement	28
9.27.4. Security.....	28
9.27.5. Risks/Liabilities/Disclaimers.....	29
10. Security Incident and Event Reporting	29
10.1. Whistleblowing.....	30
10.2. Requests for Legal Holds and 3 rd Party Subpoenas.....	30
11. Compliance	30
12. Enforcement.....	31
13. Key Roles & Responsibilities	31
14. Reference Material.....	32
15. Exception(s):.....	32
16. Revision History:	33