

<b>Title:</b> Modern Hire Product & Software Development Lifecycle	
<b>Department:</b> Information Security	<b>Contact:</b> Jamie Macko
<b>Approval Date:</b> 11/2022	<b>Last Review Date:</b> 11/2022 <b>Review Period:</b> Annual
<b>Applicability:</b> 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.	
<b>Authority:</b> 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. Overview.....	3
2. Purpose.....	3
3. Scope.....	3
4. Development Lifecycle.....	3
4.1. Roadmap and backlog.....	4
4.2. Requirement Specification.....	4
4.3. Build Sprints .....	4
4.3.1. Documentation .....	4
4.3.2. Design and Coding Standards .....	4
4.3.3. Product and Software Assurance .....	5
4.3.4. Capacity Planning .....	5
4.3.5. Software Updates .....	6
4.3.6. Final System Validation on Pre-production .....	6
4.3.7. Release to Production.....	6
4.3.8. Production Support .....	6
4.3.9. Retirement.....	6
4.3.10. Retirement Security Review & Data Destruction .....	6
5. Environments for Development and Production Testing.....	6
5.1. Beta – Construction Environment.....	7
5.2. Test.....	7
5.3. UAT – User Acceptance Testing Environment .....	7
6. Enforcement of SDLC Process .....	7
6.1. Requirements Reviews.....	7

- 6.2. Security and Data Privacy..... 7
- 6.3. 508 and Web Content Accessibility Guidelines Level A Compliance ..... 7
- 7. About the Microsoft Security Development Cycle..... 8
- 8. Microsoft SDL Optimization Model..... 8
- 9. SDL Applicability..... 8
- 10. Roles, Responsibilities, and Qualifications of Security Personnel ..... 8
- 11. Simplified SDL Security Activities ..... 9
  - 11.1. Security Activities..... 10
    - 11.1.1. SDL Practice 1: Training Requirements ..... 10
    - 11.1.3. SDL Practice 3: Deprecate Unsafe Functions..... 11
    - 11.1.4. SDL Practice 4: Static Analysis ..... 11
    - 11.1.5. SDL Practice 5: Manual Code Review ..... 11
    - 11.1.6. SDL Practice 6: Penetration Testing..... 11
    - 11.1.7. SDL Practice 7: Vulnerability Analysis of Similar Applications ..... 11
- 12. Other Process Requirements ..... 12
  - 12.1 Root Cause Analysis..... 12
  - 12.2 Periodic Process Updates..... 12
- 13 Application Security Verification Process ..... 12
- Appendix A: SDL Process Illustration..... 13
- Enforcement..... 13
- Key Roles & Responsibilities ..... 13
- Reference Material ..... 14
- Exception(s):..... 14