

ISO/IEC 19678:2015-05 (E)

Information Technology - BIOS Protection Guidelines

| Contents | | Page |
|--------------------|---|-------------|
| Foreword | | v |
| Introduction | | vi |
| 1 | Scope | 1 |
| 2 | Conformance | 1 |
| 3 | Normative references | 2 |
| 4 | Terms and definitions | 2 |
| 5 | Symbols (and abbreviated terms) | 3 |
| 6 | Background | 4 |
| 6.1 | System BIOS | 4 |
| 6.2 | Role of System BIOS in the Boot Process | 5 |
| 6.3 | Updating the System BIOS | 8 |
| 6.4 | Importance of BIOS Integrity | 8 |
| 6.5 | Threats to the System BIOS | 9 |
| 7 | Threat Mitigation | 10 |
| Bibliography | | 14 |