

# ISO/IEC 29147:2014-02 (E)

## Information technology - Security techniques - Vulnerability disclosure

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Abbreviated terms .....	2
5	Concepts .....	3
5.1	General .....	3
<b>Vulnerability handling processes .....</b>		<b>3</b>
5.3	Products and online services .....	5
5.4	Stakeholders .....	6
5.5	Vulnerability disclosure process summary .....	7
5.6	Information exchange during vulnerability disclosure .....	8
5.7	Confidentiality of exchanged information .....	9
5.8	Vulnerability advisories .....	9
5.9	Vulnerability exploitation .....	9
6	Vulnerability disclosure policy considerations .....	10
6.1	General .....	10
6.2	Minimum policy aspects .....	10
6.3	Optional policy aspects .....	11
7	Receipt of vulnerability information .....	12
7.1	General .....	12
7.2	Potential vulnerability report and its secure receiving model .....	12
7.3	Acknowledgement of receipt from finder or a coordinator .....	12
7.4	Tracking incoming reports .....	12
7.5	On-going communication with finder .....	12
7.6	Detailed information .....	12
7.7	Support from coordinators .....	13
8	Possible vulnerability reporting among vendors .....	13
8.1	General .....	13
8.2	Typical cases calling for vulnerability reporting among vendors .....	13
8.3	Reporting of vulnerability information to other vendors .....	13
9	Dissemination of advisory .....	14
9.1	General .....	14
9.2	Purpose of advisory .....	14
9.3	Consideration in advisory disclosure .....	14
9.4	Timing of advisory release .....	14
9.5	Contents of advisory .....	15
9.6	Advisory communication .....	16
9.7	Advisory formats .....	17
9.8	Advisory authenticity .....	17

<b>Annex A (informative) Details for handling vulnerability/advisory information .....</b>	<b>18</b>
<b>Annex B (informative) Sample policies, advisories, and global coordinators .....</b>	<b>26</b>
<b>Bibliography .....</b>	<b>34</b>