



**ISO/IEC 29151:2017**

**信息技术 安全技术 个人身份信息保护实践规范**

(海德认证内部翻译稿)

查阅全文请联系北京海德国际认证有限公司

联系电话：010-84905056，010-65817800

邮箱地址：[common@hicchina.com.cn](mailto:common@hicchina.com.cn)

北京海德国际认证有限公司

发布日期：2017-08-18

实施日期：2017-08-18

---

# 目录

前言.....	5
引言.....	6
<b>1 范围</b> .....	<b>9</b>
<b>2 规范性引用文件</b> .....	<b>9</b>
<b>3 术语和定义</b> .....	<b>9</b>
3.1 定义.....	9
3.2 缩略语.....	9
<b>4 概述</b> .....	<b>10</b>
4.1 个人信息（PII）保护目标.....	10
4.2 个人信息（PII）保护要求.....	10
4.3 控制措施.....	11
4.4 控制措施的选择.....	11
4.5 制定组织特定指南.....	12
4.6 生命周期考量.....	12
4.7 本规范的结构.....	12
<b>5 信息安全策略</b> .....	<b>13</b>
5.1 信息安全管理方向.....	13
<b>6 信息安全组织</b> .....	<b>13</b>
6.1 内部组织.....	13
6.2 移动设备与远程办公.....	16
<b>7 人力资源安全</b> .....	<b>16</b>
7.1 雇佣前.....	16
7.2 雇佣期间.....	16
7.3 雇佣终止与变更.....	17
<b>8 资产管理</b> .....	<b>17</b>
8.1 资产责任.....	17
8.2 信息分类.....	19
8.3 介质处理.....	20

---

<b>9 访问控制</b>	21
9.1 访问控制的业务要求	21
9.2 用户访问管理	21
9.3 用户责任	22
9.4 系统与应用访问控制	23
<b>10 密码术</b>	24
10.1 密码控制措施	24
<b>11 物理与环境安全</b>	24
11.1 安全区域	24
11.2 设备	24
<b>12 运行安全</b>	25
12.1 运行程序与责任	25
12.2 恶意软件防护	26
12.3 备份	26
12.4 日志记录与监控	27
12.5 运行软件控制	28
12.6 技术漏洞管理	28
12.7 信息系统审计考量	28
<b>13 通信安全</b>	29
13.1 网络安全管理	29
13.2 信息传输	29
<b>14 系统获取、开发与维护</b>	30
14.1 信息系统安全要求	30
14.2 开发与支持过程中的安全	30
14.3 测试数据	31
<b>15 供应商关系</b>	31
15.1 供应商关系中的信息安全	31
15.2 供应商服务交付管理	33
<b>16 信息安全事件管理</b>	33
16.1 信息安全事件管理与改进	33

---

<b>17 业务连续性管理中的信息安全方面</b> .....	35
17.1 信息安全连续性.....	35
17.2 冗余 .....	35
<b>18 合规性</b> .....	36
18.1 遵守法律法规与合同要求.....	36
18.2 信息安全审查.....	37
<b>附录 A 个人信息（PII）保护扩展控制集</b> .....	39

