

面向交易对方 信息安全基准

Ver. 2.11

2019年3月1日

松下电器产业株式会社

全球采购公司

信息安全部

<目 录>

I. 松下集团的信息安全基本方针

II. 签订保密合同

III. 交易对方信息安全基准

1. 目的

2. 适用

3. 对交易对方的信息安全要求事项

4. 详细的要求事项

(1) 信息安全管理体制的确立

(2) 信息资产的机密管理

(3) 人的对策

(4) 信息安全事件/事故处理

(5) 信息安全管理实施

附则

I. 松下集团的信息安全基本方针

松下电器产业株式会社以及相关公司（以下，称作“本公司”）的目标在于，按照经营基本方针，通过卓越的技术、产品以及服务，使顾客满意并取得顾客的信赖。因此，我们要认识到以顾客的信息、个人信息、财产信息为首的信息的保护是非常重要的，我们应将信息安全定位为经营的重要战略之一，按照以下内容推进信息安全工作，努力实现健全的信息化社会。

1. 信息安全体制

在各组织确立信息安全的责任体制，通过制定和实施必要的规程，进行适当的管理。

2. 信息资产的管理

为了确保信息的安全，要根据信息的重要性及其风险明确处理方法，进行适当的管理。

3. 教育和培训

对全体董事以及员工，要持续实施信息安全相关教育和培训，以期提高信息安全意识并贯彻信息安全相关各规程。对于违反规程者，要加以惩戒，严肃处理。

4. 提供可让顾客放心的产品和服务

考虑到被使用的顾客信息的安全，努力做到提供令顾客放心的产品和服务。

5. 遵守法令和持续改善

在遵守相关法令和其它的规范的同时，根据环境的变化持续地加以改善和提高，以确保信息安全。

II. 签订保密合同

本公司和交易对方共享机密信息时，需签订包含下列的保密条款在内的基本交易合同或单项合同。

- a.) 保密义务
- b.) 成为保密对象的信息的范围
- c.) 保密义务期限(也包含无限期)
- d.) 使用目的的限制
- e.) 访问者仅限业务上有必要了解该信息的人员
- f.) 机密信息的管理方法
- g.) 机密信息的复制/复写的限制
- h.) 保密期满后的归还或废弃的规定
- i.) 本公司就保密状况进行确认(提问或监察等)的措施的规定
- j.) 违反合同时的措施(应加入损害赔偿、以及禁止市场流通、销售的条款等)
- k.) 禁止擅自进行二次委托
- l.) 禁止将个人所有的电脑用于业务之上

III. 交易对方信息安全基准

1. 目的

本公司作为以实现健全的信息化社会为目标的全球性企业，通过推进合理的信息安全，及正确地处理和管理顾客信息、个人信息、技术/质量/产品/服务等方面的信息资产，旨在履行企业的社会性责任，因此本基准也同时要求与本公司共享机密信息的交易对方实施合理的信息安全对策。

通过构建可正确管理和利用信息的环境，使本公司以及交易对方能够放心、安全且高效地开展工作，实现事业的持续稳定发展和共同繁荣。

2. 适用

本基准适用于与本公司共享指定机密信息的交易对方处理、管理该当信息以及与该信息相关的业务（技术转让/业务委托/资材采购活动等）全盘。

适用的对象信息是，包括与本公司共享的机密信息以及利用该信息创造出的机密信息。

适用对象的机密信息的形态包括记载机密信息的纸张（文件、图纸等）（以下、称作「纸质」）、电子化信息、化体了机密信息的物体（以下、称作「化体品」）、技术经验等所有形态。

关于须进行更加严格管理的绝密信息和重要信息等，还需适用备忘录/保密合同等追加管理对策。

3. 对交易对方的信息安全要求事项

对交易对方的要求事项具体有下述的（1）到（5）项。

而且，针对本基准的要求事项，如果交易对方的信息管理达不到本公司要求水平时，我们会采取相应措施限制与该交易对方实行机密信息共享。因此，请实施下述要求事项。

- （1） 信息安全管理体制的确立
构建能够有组织性地推进信息安全的体制。
 - （1-1） 构建信息安全管理组织体制
 - （1-2） 制定信息安全工作的基本思想及规则
- （2） 信息资产的机密管理
明确须进行机密管理的信息，并实施必要的管理。
 - （2-1） 机密信息的明确化
 - （2-2） 机密信息的交换/归还的管理

- (2-3) 物理性管理
- (2-4) 信息系统用户 ID 和密码的管理
- (2-5) 电脑/服务器等信息系统的设置/运用以及废弃的管理
- (2-6) 非法程序的对策
- (2-7) 备份的实施
- (2-8) 与贵公司共享机密信息的委托对象的管理

- (3) 人的对策
 - 实施保密誓约等、防止信息泄漏的人为性对策。
 - (3-1) 实施信息安全的启蒙、教育及培训
 - (3-2) 向员工等取得保密誓约书
- (4) 信息安全事件/事故处理
 - 将发生事件/事故时的处理方法实现明确化，并实施。
 - (4-1) 事故报告和处理体制的确立
 - (4-2) 事故处理流程的明确化
- (5) 实施信息安全管理
 - 实施信息安全管理，以便于持续推进改善工作。
 - (5-1) 定期确认有组织性的信息安全工作的实施情况
 - (5-2) 依据确认结果实施改善工作

4. 详细的要求事项

“3. 对交易对方的信息安全要求事项”中所记述的各个要求事项，下面将进行更加详细的说明。
以下、将交易对方称作「贵公司」。

(1) 信息安全管理体制的确立

1-1	构建管理信息安全的组织体制，明确具体责任和职责，并文档化。
1-2	制定信息安全工作的基本思想(方针)及规则，并文档化。

(2) 信息资产的机密管理

(2-1) 机密信息的明确化

2-1-1	请制作机密信息的资产清单以确定资产，并请定期更新该资产清单。
2-1-2	按照合同要求对机密信息进行了复制/复写时，请对复制/复写件也实施与机密信息原件等同的安全管理。
2-1-3	请将机密信息与除此之外的信息明确区分并实行管理。

(2-2) 机密信息的交换/归还的管理

2-2-1	请依据与本公司协商一致的规则进行机密信息的交换。
2-2-2	请制定带出机密信息的规则，并实施下述 a)-d) 的所有该当要求事项。 a.) 带出机密信息时，请取得管理责任人的许可。 b.) 带出过程中，务必要将机密信息常时随身携带，不得离开自己视线范围。 c.) 将机密信息保管到电脑/便携信息终端/记忆媒体里带出、或者用电子邮件附加发送时，务必要实施加密。 d.) 带出化体品(模具/试制品等)时，采取遮盖措施避免让外部人员看到。
2-2-3	当受本公司委托的业务结束后，请用与本公司协商一致的流程归还机密信息。如果是在贵公司废弃机密信息时，请按照经本公司同意方法，实施下述 a)-d) 的所有该当要求事项。并按照本公司提出的要求，提供该废弃记录。 a.) 如果是电子化信息时，请将服务器、电脑、便携信息终端、记忆媒体等里保管的机密信息全部删除。 b.) 如果是纸质(文件/图纸等)时，请用碎纸机裁剪、或溶解、焚烧等方式处理。 c.) 如果是化体品(模具/试制品等)时，请破坏至无法读取原信息。 d.) 如果向专业废弃物处理公司等外部公司委托废弃时，请签订保密合同。

(2-3) 物理性管理

2-3-1	为限制无关人员随便进入处理机密信息的场所(公司厂房用地/建筑物/房间内)，请采取相关的物理性对策。
2-3-2	处理机密信息的场所仅限业务上有必要的人员方可进入，而且请取得管理责任人的许可。
2-3-3	请确立能够在公司里区别员工和外部来访人员的体制。
2-3-4	对处理机密信息的场所的进出，请取得进出房间的双向记录或者单向记录(包括监视摄像机图像)，并定期确认该记录是否正确取得。
2-3-5	在处理机密信息的场所，禁止带入个人所有的电脑、手机、便携信息终端、记忆媒体(SD卡、USB 媒体等)、通信设备(无线 LAN 等)等。如果需要带入时，请实施下述 a) 及 b) 的要求事项。 a.) 需要带入时，请事前取得管理责任人的许可。 b.) 即使允许带入时，也须制定禁止连接公司电脑或公司内部网络、禁止使用手机、便携信息终端的照相功能等相关规则，以实施合理管理。
2-3-6	针对纸质信息(文件/图纸等)/化体品(模具/试制品等)，仅限业务上有必要获知信息的人员可以处理，并实施防盗对策。

(下述的 2-4 到 2-7 项，当持有本公司提供的电子化信息的情况下为实施对象)

(2-4) 信息系统用户 ID 和密码的管理

2-4-1	请制定信息系统的用户 ID 的管理规则，实施下述 a)-d) 的所有要求事项。 a.) 采取相关措施制止信息系统用户与其他用户共享 ID。 b.) 制定信息系统的用户 ID 发行流程和认可流程。 c.) 由于离职或调动等与相关业务无关人员的 ID、以及临时性使用的 ID 等，不再需要的 ID 及时删除。 d.) 定期实施确认，确保不存在未管理的 ID。
2-4-2	请制定密码的管理规则，实施下述 a)-c) 的所有要求事项。 a.) 密码必须设定成他人难以推测的形式。 b.) 密码必须定期变更。 c.) 密码必须实行保密性管理，不得让他人随意获知。
2-4-3	构建相关体制，对保管了机密信息的服务器实行访问限制，仅限业务上有必要获知信息的人员方可访问。
2-4-4	请取得访问机密信息的人员的记录(日志)，并在与本公司协商一致的期间内进行合理保管。

(2-5) 电脑/服务器等信息系统的设置/运用以及废弃的管理

2-5-1	公司内部网络务必要通过路由器、防火墙等实行与公司外部网络(因特网)分离。
2-5-2	制定引进/设置电脑、便携信息终端、服务器的具体规则，并加以实施。
2-5-3	请将机密信息保管在服务器里。服务器须实施合理的安全管理。
2-5-4	请采取措施制止个人所有电脑、个人用便携信息终端、及个人所有记忆媒体用于业务之上。
2-5-5	制定包含下述内容在内的电脑、便携信息终端、服务器、记忆媒体的废弃/再使用规则，并加以实施。 · 为防止原数据被还原，请制定彻底删除硬盘内的信息或物理性毁坏硬盘的规则。
2-5-6	保管了机密信息的服务器，请设置到可以确保安全的合理场所，并实施下述 a) 及 b) 的要求事项。 a.) 对服务器的设置场所的出入，仅限业务上有必要的人员。 b.) 对服务器实施防盗对策。

(2-6) 非法程序对策

2-6-1	请制定防电脑病毒和非法程序的相关对策，并实施下述 a)-d) 的所有要求事项。 a.) 引进系统管理责任人指定的防病毒软件(种类/版本等)。 b.) 在电脑中安装防病毒软件、使其处于常时运作且可防御病毒的状态。 c.) 定期更新病毒定义文件。 d.) 对于保管的所有文件，定期实行病毒扫描。
2-6-2	请制定能够将病毒危害控制于最小限度的对策(感染病毒时的物理性处理方法或报告/通知/处理方法等)，并加以实施。
2-6-3	禁止安装/使用文件交换软件(BT、电驴等信息泄漏风险较高的软件)，并请定期进行确认。
2-6-4	禁止通过免费邮件(Yahoo 邮件等)及数据共享服务(百度文库等)实行机密信息的发送/共享。

(2-7) 备份的实施

2-7-1	针对备份的必要性/频度，经与本公司研讨决定需要取得备份时，请制定电子化机密信息的备份规则，并加以实施。
2-7-2	请制定备份数据的保管规则，并按照机密区分实施合理管理。

(下述 2-8 项，当存在与贵公司共享机密信息的委托对象时为实施对象)

(2-8) 与贵公司共享机密信息的委托对象的管理

2-8-1	贵公司与委托对象共享机密信息时，请在事前书面通知本公司该事实。
2-8-2	请贵公司与您的共享机密信息的委托对象签订包括下述 a)-l) 条款的保密合同 (或者是包括保密项目在内的合同)，具体制定机密信息的处理及交换相关规则，并实施管理。 a.) 保密义务 b.) 成为保密对象的信息的范围 c.) 保密义务期限 (也包含无限期) d.) 使用目的的限制 e.) 访问者应限定为在业务上有必要了解该信息的人员 f.) 机密信息的管理方法 g.) 机密信息的复制/复写的限制 h.) 保密期限期满后的归还或废弃的规定 i.) 保密相关事项确认 (提问和监查等) 措施的规定 j.) 违反合同时的措施 (应加入损害赔偿、以及禁止市场流通、销售的条款等) k.) 禁止擅自进行二次委托 l.) 禁止用个人所有电脑处理业务
2-8-3	向与贵公司共享机密信息的委托对象发送电子化机密信息时，请将该当文件实施加密。
2-8-4	与贵公司共享机密信息的委托对象之间实行机密信息的交换时，请留取记录并实行管理。
2-8-5	请要求与贵公司共享机密信息的委托对象，向其员工取得与贵公司的员工相同的保密誓约书。
2-8-6	请要求与贵公司共享机密信息的委托对象，实施与贵公司同等水平的信息安全管理，并对其实况进行定期确认。
2-8-7	请要求与贵公司共享机密信息的委托对象，对其员工实施信息安全教育。

(3) 人的对策

(3-1) 实施信息安全的启蒙、教育和培训

3-1-1	请对全体员工定期实施信息安全教育。
3-1-2	请对管理责任人定期实施信息安全教育。
3-1-3	通过全体员工实施自我点检等，以定期确认信息安全相关规则的遵守状况。如果存在不符合事项时，请管理责任人负责指示改善工作。
3-1-4	面向全体□ 工□ 施目□ 型攻□ 的教育或培□。

(3-2) 向员工等取得保密誓约书

3-2-1	在就业规则中设定保密相关的条款，并请向员工取得保密誓约书。
3-2-2	如果任用派遣员工时，请向其取得相关保密誓约书。

(4) 信息安全事件/事故处理

(4-1) 确立事故报告/处理体制

4-1	选任发生事故时的联络/处理责任人，确立包含下述 a)-c) 事项在内的事故报告体制。 a.) 发现了信息安全上的问题及有发生的可能时，或者目击了事件/事故及其迹象时，请迅速向管理责任人报告。 b.) 针对本公司信息，如果发生了上述问题，请在与本公司协商一致的时间内迅速向本公司报告。 c.) 遭受目标型攻击致使本公司相关信息的设备感染病毒时、在与本公司协定的时间内向本公司报告。
-----	--

(4-2) 事故处理流程的明确化

4-2	明确了包括下述 a)-f) 的事项在内的信息安全事故处理流程，并在组织内彻底贯彻。 a.) 把握受害状况和使受害影响最小化的紧急处理 b.) 原因调查和暂定措施 c.) 信息泄露时，采取向相关第三方报告等、相关人员能够进行自卫和处理的措施。 d.) 必要时，公关对应处理，向相关政府机关报告 e.) 事故的经过、处理经过的记录 f.) 构建可以实施防止再发生对策和彻底贯彻的体制
-----	---

※信息安全事故的范例：

信息(文件、电脑、记忆媒体、化体品等)的被盗/丢失、信息的泄露、电子邮件/传真错误传送、对信息非法访问、非法获取、丧失可用性(系统故障、数据被破坏等)、丧失完整性(数据被篡改、删除)等

(5) 信息安全管理实施

(5-1) 定期确认有组织性的信息安全工作的实施情况

5-1	请定期确认有组织性的信息安全推进工作的实施情况。
-----	--------------------------


(5-2) 依据确认结果实施改善工作

5-2	对于确认结果中明确化的不符合事项，请制定改善计划并实施改善。
-----	--------------------------------

附则

1. 施行日期 2019年3月1日
2. 适用本基准的机密信息的指定方法

标示范例

 <p>A red rectangular box containing the text: 秘 Confidential 直到: 为止</p>	<p>按照 1~3 中的任意一种方法进行指定。</p> <ol style="list-style-type: none">1. 在文件、图纸、文件夹、电子数据等上标示了“秘 Confidential”的信息。2. 在电子形式的文件名称上标注了“秘-文件名称”或者“C-文件名称”的信息。3. 本公司另行指定为机密信息的信息。
---	---

3. 检查表

请使用「面向交易对方 信息安全基准检查表」定期实施自我检查，并按照本公司要求进行报告。