第二节：信息安全 之　人力资源

1、组织架构

现状描绘：口号很丰满，执行很骨感；制度很完备，结局很悲催。

必要的投入，这是信息安全的基础。如果贵公司人员也不愿意配、钱也不乐意出。那么就另当别论了。

您可以先考虑一下：

信息安全谁负责？谁主导？

信息安全的制度谁制定、落实、监督？

答案可能是：

信息安全的各个环节和因素应该分配到内部各个职能部门中。

入职调查、工资组成（保密津贴）等由谁完成？

产品宣传（网站、展会）由谁完成？

文档权限、打印、邮件、归档、网络管控、应用系统服务、代码、图档、BOM？

明确监管责任部门，普遍的现象，责任很明确，权责不清晰。给你天大的责任，屁大的权限。最好是屁都不要放啦。

平时修修电脑、拔拔网线，业务部门提什么需求就要无条件满足。美其名曰：IT 服务于业务，仅仅是一个服务者，咸鱼何时翻身呢？

这些背黑锅的责任部门没有任何否决权？最后所谓的信息安全都是空谈。

（不好意思，我把日常工作简单化了，可能还有更多技术含量高的事情在做。）

可能的对策：

a、部门权责对等？

b、关键节点统一管理？

（如 涉密资料统一管控、网络、邮件、外发、打印等等集中管控）

c、违反原则、底线 坚持说 “不”？

（没有这个权限和勇气？赶快打道回府吧！）

组织结构就保密了。

Review:

对于信息安全来说，必提 ISO 27000、《等保》，一定会有风险管控（风险分析、差距测评）、体系建设等等。

《信息系统安全等级保护基本要求》等系列文档 是中国国家推荐标准。

ISO 27001 共有 133 个控制点，39 个控制措施，11 个控制域。其中 11 个控制域包含如下：

1)安全策略、2)信息安全的组织、3)资产管理、4)人力资源安全、5)物理和环境安全、6)通信和操作管理、7)访问控制、8)系统采集、开发和维护、9)信息安全事故管理、10)业务连续性管理、11)符合性

如果您要冒充牛 XX 的人，也可以随随便便说一说。

2、 人员安全

很多人认为 人员如何安全？跟 信息安全没有必然的联系？入职后才会涉及到安全层面的考虑。

抛出如下问题：

a、此员工存在劳动纠纷或者争议？

b、此员工与前公司有保密协议、竞业限制协议？

c、特殊岗位的约束文本、背景调查？

那么如何保证 此员工 之前的纠纷不轻易带入新的公司呢？最大限度的保护公司的信息安全呢？

此刻让我想起：消防安全工作以预防为主、防消结合。在企业中我们何尝不是扮演消防员的角色？

不好意思，这些都需要白纸黑字留存归档的。作用是什么？

您懂的：害人之心不可有，防人之心不可无。

新员工入职承诺书

新员工入职承诺书

本人就入职[redacted]（以下简称“公司”），特向公司承诺如下：

一、本人严格遵守与公司签署的《保密协议》中所有条款及相关保密制度，如有违反，公司可视情节轻重及损失大小要求本人予以经济赔偿，直至无偿解聘与提请法律诉讼。

二、出勤规定

某岗位承诺书（部分内容截取）

采购员承诺书

1、廉洁自律，严守工作纪律，不向供应商索贿、受贿。

2、不接受供应商礼金、有价证券、礼品（价值 100 元以上）、宴请、报销费用、提供旅游、报销应由本人及配偶、子女支付的个人费用等变相行贿行为，确实难以拒绝的应上报公司处理。

3、在[redacted]工作期间，愿意随时接受公司调查或审计。

4、离任或离职前，愿意配合公司进行离任或离职审计。

5、离职后，在法律许可的追诉期内，愿意配合公司对本人在职期间内的工作进行调查。

以上承诺本人坚决做到有诺有践，请公司和所有员工对我进行监督，本人愿意随时接受公司调查、审计，如有违诺行为，愿意接受公司依法依纪处理。

承诺人：

保密协议（部分内容截取）

第四条　保密范围

甲方应保密的范围包括但不限于以下内容：

1、甲方在任职期间开始前所持有的合法科研成果、技术秘密或商业秘密已被应用于 AIC 项目之中的部分；

2、甲方在任职期间内所获得的、与 AIC 项目相关的科研成果、技术秘密或商业秘密。

3、甲方在任职期间直接或间接获取的、乙方原先已有的和陆续获得的科研成果、技术秘密或商业秘密，而无论其是否在甲方工作范围之内。

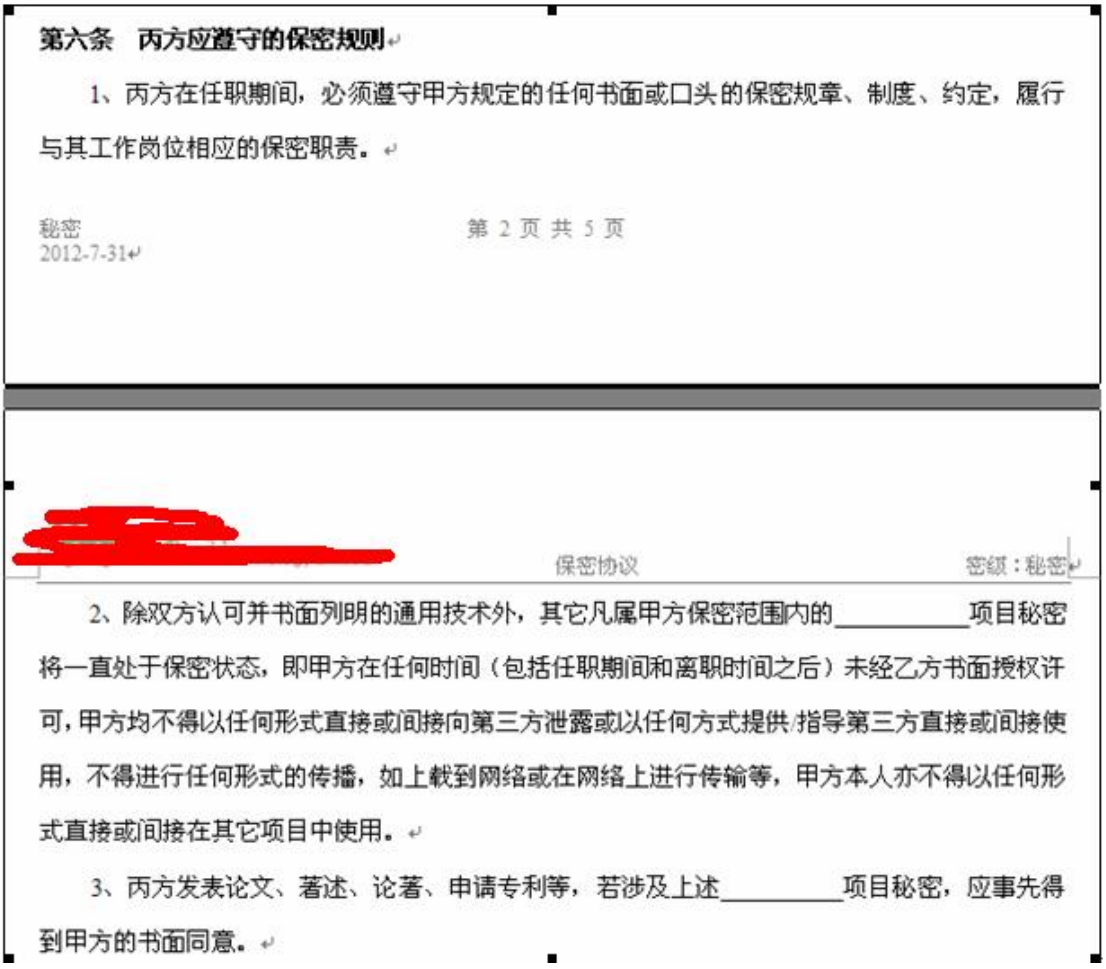
上述科研成果、技术秘密和商业秘密包括但不限于任何计算机程序、代码、算法、公式、过程、观念、图表、照片、制图、设计思路、方案、设计草图、结果、专门试验或检测装置、样品、半成品、成品、加密方法、发明创造（包括发明、实用新型和外观设计，而无论其是否获得专利）、技术诀窍、标准化方案和文件、相关著述、版权、商标、产品研发计划、预测、策略、规范、实际或潜在商业活动的信息、客户与供应商名单、财务事项、市场情报、营销计划等商务信息。此外，还包括任何形式的技术总结、会议记录、工作记录、工作笔记、讨论内容，以及检索到的现有技术或信息、利用的现有技术或信息以及对现有技术或信息的整理、分析或总结。

以上保密范围所涉秘密信息统称“_____项目秘密”。

第五条 知识产权归属

1、丙方在任职期间内，所取得的任何与甲方项目有关的技术成果，均视为履行职务或者利用甲方资源完成的职务成果，其知识产权均归甲方所有，但丙方享有国家相关法规规定的职务发明人权益。

2、在上述知识产权获取和使用过程中，丙方有责任依甲方要求协助丙方获取和行使相关知识产权。



第六条　丙方应遵守的保密规则

1、丙方在任职期间，必须遵守甲方规定的任何书面或口头的保密规章、制度、约定，履行与其工作岗位相应的保密职责。

秘密　　第 2 页 共 5 页
2012-7-31

[redacted]　　保密协议　　密级：秘密

2、除双方认可并书面列明的通用技术外，其它凡属甲方保密范围内的_____项目秘密将一直处于保密状态，即甲方在任何时间（包括任职期间和离职时间之后）未经乙方书面授权许可，甲方均不得以任何形式直接或间接向第三方泄露或以任何方式提供/指导第三方直接或间接使用，不得进行任何形式的传播，如上载到网络或在网络上进行传输等，甲方本人亦不得以任何形式直接或间接在其它项目中使用。

3、丙方发表论文、著述、论著、申请专利等，若涉及上述_____项目秘密，应事先得到甲方的书面同意。

第九条　保密费和竞业限制补偿

双方约定，在甲方直接或通过乙方支付给作为自然人的丙方报酬中，已包括丙方在职期间以及离职后所有应得的保密费用和竞业限制补偿，甲方无须为此另外支付任何费用或补偿。

制度－保密管理制度（如下为摘录部分章节）

2.0 涉密信息

在公司经营活动中和员工工作中形成的、一旦泄露给第三人可能对公司利益造成损害的文字、数据、图形、实物等，统称涉密信息。

涉密信息包括但不限于以下方面内容：

A. 公司重大决策中的秘密事项或内容；
B. 公司研发产品过程中产生的技术资料、文档、记录、草案；
C. 公司尚未付诸实施的经营战略、经营方针、经营政策、经营规划、经营项目及各种经营决策；
D. 公司内部掌握的合同、协议、意向书、可行性报告、重要会议记录；
E. 公司财务预决算报告、各类财务报表、统计报表、账簿、各类财务凭证；
F. 公司市场调研报告、营销计划、客户信息及尚未决定公开的其它营销信息；
G. 公司员工人事档案、薪酬及未公开的其它人力资源资料；
H. 其它经公司确定应当保密的事项。

过、大过、辞退处分。

6.3 部门负责人的失职错误

6.3.1 各部门负责人对本部门发生的泄密事故承担连带责任

A. 本部门发生机密级保密信息泄密事故或一年内发生 3 次以上违反本规定的行为，可给予警告、记过处分；

B. 本部门发生绝密级保密信息泄密事故或一年内累积获 2 次警告者，可根据情节轻重给予记过、大过处分；

C. 本部门发生泄密事故并造成损失者，作为连带责任人，赔偿损失额的 30%。

6.3.2 信息部负责人对公司内发生的泄密事故承担连带责任

A. 公司发生机密级保密信息泄密事故，可给予警告处分；

B. 发生绝密级保密信息泄密事故，可给予记过处分；

C. 公司因泄密事故遭受损失，作为连带责任人，赔偿损失额的 10%。

6.4 其它

A. 在信息保密方面发生隐瞒不报、掩盖错误、弄虚作假、营私舞弊等行为时，不论情节轻重，相关人员一律予以辞退。造成公司损失者，追究其经济、法律责任；

B. 违法其它保密制度规定者，可根据情节轻重情况，给与批评、警告、记过、大过、辞退处分，并处以 50-5000 元罚款。

7.0 管理授权

本制度由信息部负责解释并监督执行。信息部负责人拥有以下权力：

A. 知情权：信息部负责人可随时了解公司信息安全执行情况，全体员工均应服从询问并予以配合。

B. 检查权：信息部负责人可随时以合法手段检查公司保密制度及相关规定执行情况，全体员工均应服从检查并予以配合。

C. 评价权：信息部负责人可对部门和员工在信息保密方面的表现做出评价，该评价将影响部门和员工业绩考核的总评分。

D. 处罚权：信息部负责人可依据本制度第 6.0 条，对违反本规定和造成泄密事故的行为提出处罚建议，报公司领导批准后交由相关部门执行。

3、意识培养

安全重要，意识先行。如何培训。采用什么途径、方式、方法？可谓八仙过海各显神通。

如何把这种安全意识变成行为性习惯？

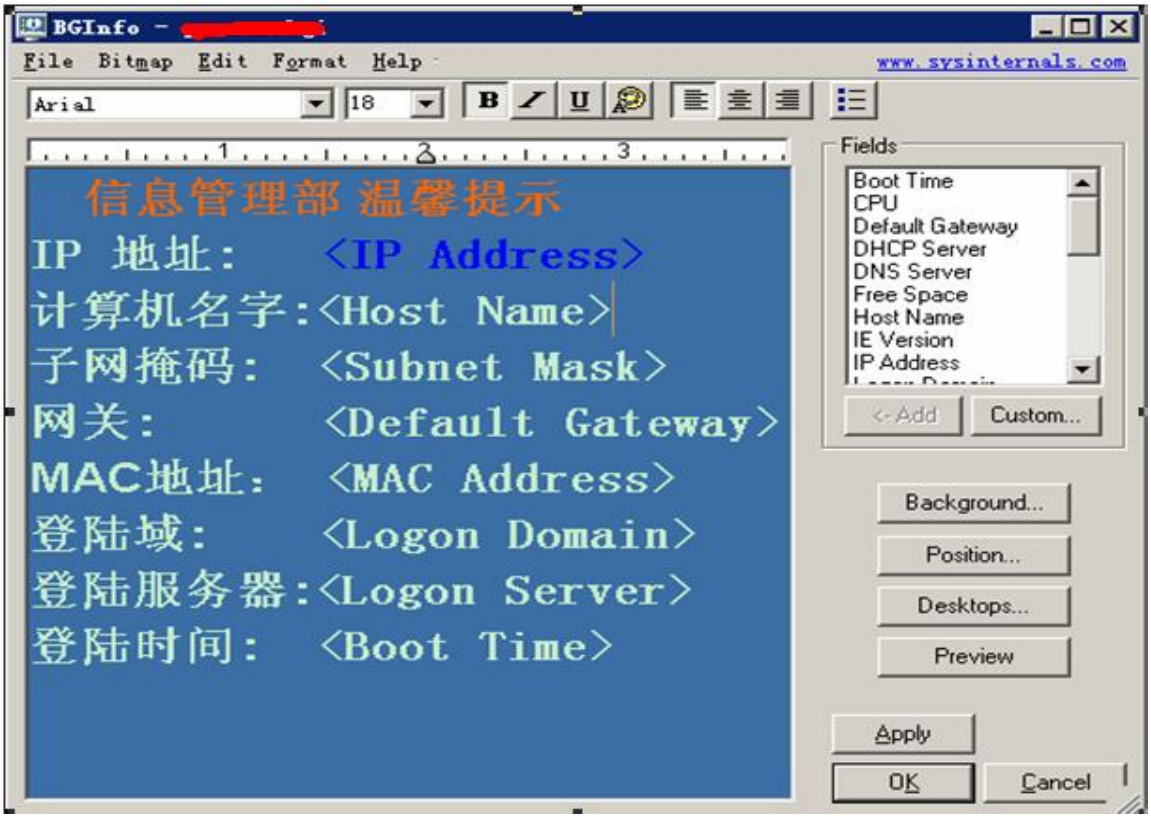
如：

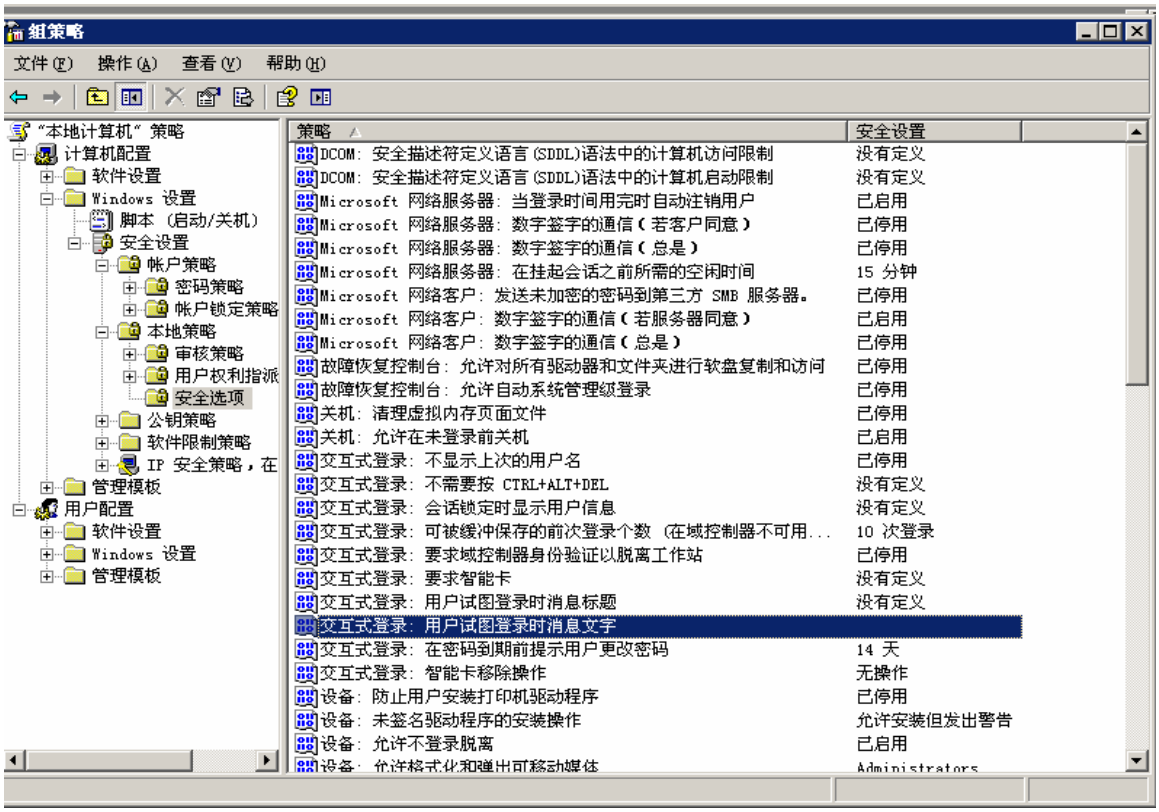
制度、培训层面：

a、入职培训(制度的说明、解释、过往案例的介绍)

技术层面：

a、宣传（统一修改桌面提示信息、网站宣传、开机登录提示、FLASH 宣传等等）





Review:

关于技术管理层面的配合措施，后续会有专门篇幅进行说明。