业务通知单

制发单位：安全管理部　　签发：黄虎　2018 年 9 月 21 日

编号	中电信沪安管业〔2018〕32号	缓急	普通	密级	
主送单位	各单位、各部门				
抄送单位	上海通服				
任务事项（标题）	**关于开展全员网络与信息安全基本常识普及培训的通知**				

近期，媒体相继报道了浙江警方破获30亿条数据泄露案件、华住集团5亿条数据泄露事件、英国航空网站38万条数据泄露事件等，涉案数据之多、规模之广，数据安全问题再次引发舆论和社会强烈关注。根据公司司务会精神，为落实好企业用户信息保护相关工作，进一步增强全体员工的网络信息安全意识，安全管理部编写了《上海电信及外包合作方员工网络与信息安全基本常识》（以下简称网信安基本常识，见附件1），现随文下发，请各单位、各部门组织做好普及培训。有关要求通知如下：

一、时间安排

(一) 学习宣贯阶段（9 月 21 日至 10 月 20 日）

1、各单位/部门通过办公会议、专题会议、班组学习等多种形式开展网信安基本常识培训，至少组织一次集中学习，留存培训记录。

2、培训须覆盖到各单位/部门的每一位员工（含合同制、派遣制、外包合作方），留存培训记录。

(二) 培训考核阶段（10 月 21 日至 31 日）

公司全体员工（含合同制、派遣制、外包）通过“微学院”APP 开展线上培训考核，微学院 APP 下载：http://dwz.cn/westudy，二维码如下：

二、请各单位/部门高度重视本次普及培训工作，统一部署、精心组织、全面覆盖、务求实效。各单位/部门员工（含合同制、派遣制、外包合作方）的参与率、合格率、优秀率作为加分项纳入本年度信息安全履职考核（在原有 15 分总分之外，额外配分 1 分）。加分细则说明如下：

(一) 有外包合作方员工的单位/部门，加 0.1 分；无外包合作方员工的单位/部门，不加分。

(二) 参与率（配分 0.3 分）=实际参与人数/应参与人数*100% 。

参与率	加分分值
100%	0.3 分
100%＞X≥95%	0.2 分
95%＞X≥90%	0.1 分
＜90%	0

(三) 合格率（配分 0.3 分）=合格人数/实际参与人数*100%，80 分为合格（满分 100 分）。

合格率	加分分值
100%	0.3 分
100%＞X≥95%	0.2 分
95%＞X≥90%	0.1 分
＜90%	0

(四) 优秀率（配分 0.3 分）=优秀人数/实际参与人数*100%，100 分为

优秀（满分 100 分）。

优秀率	加分分值
≥95%	0.3 分
95%＞X≥90%	0.2 分
90%＞X≥80%	0.1 分
＜80%	0

三、为做好线上培训考核准备，请各单位/部门全面梳理统计外包合作方员工信息（模板见附件 2），特别是具备涉及用户信息、网络数据等公司重要数据系统账号权限（包含但不仅限于：CRM、无纸化平台、客挽系统、用户信息查询系统、10000 号门户、大数据平台、认证计费系统、UDB、112 受理平台、装维移动应用等）的外包合作方员工，不漏报、不瞒报，**9 月 30 日前** OA 邮件报送安全管理部，安全管理部提交人力资源部统一开通微学院账号。

四、请资本运营部所辖合资公司、上海通服参照落实相关工作，并自行组织开展员工培训考核工作。

安全管理部联系人：

陆敏，电话：63630668，邮箱：lumin1@shtel.com.cn 。

拟稿人	姓名	陈颖
	电话	63630496

附件 1

上海电信及外包合作方员工
网络与信息安全基本常识

（一） 这些必须做

1、 做好办公计算机基础安全防护:（1）设置开机口令;（2）启用屏幕保护程序（等待时间≤5 分钟），并在恢复时使用密码保护;（3）安装并启用杀毒软件，定期（周期≤30 天）更新病毒库、进行扫描检测;（4）及时升级软件漏洞补丁;（5）不安装与工作无关的软件;（6）暂离计算机终端时主动锁屏。

2、 口令设置符合强度要求:（1）长度应至少 8 位;（2）应包括数字、小写字母、大写字母、特殊符号 4 类中至少 3 类;（3）应与用户名无相关性，口令中不得包含用户名的完整字符串、大小写变位或形似变换的字符串;（4）应避免键盘排序密码;（5）应更换系统或设备的出厂默认口令。

3、 妥善保管本人的账号、口令、密钥。

4、 保守国家秘密和企业商业秘密，不该说的秘密不说，不该问的秘密不问，不该看的秘密不看。

5、 使用公司企业内部网和邮箱传递含有商密信息、敏感信息的文件、资料。

6、 发现用户发布的信息属于法律、行政法规禁止发布或者传输的，立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

7、 遵守“七条底线”:（1）法律法规底线;（2）社会主义制度底线;（3）国家利益底线;（4）公民合法权益底线;（5）社会公共秩序底线;（6）道德风尚底线;（7）信息真实性底线。

（二） 这些不能做

1、 不得将本人的账号、口令、密钥转借他人共享使用。

2、 不得盗用他人的账号、口令、密钥。

3、 不得公开张贴账号、口令、密钥口令。

4、 不得将涉密计算机、涉密存储设备接入互联网及其他公共信息网络（“上网不涉密、涉密不上网”）。

5、 不得将含有涉密信息、敏感信息的文件、资料放置在公共打印区、公共办公区、公共休息区等不受控区域。

6、 不得通过公共互联网或移动互联网（含微信、易信、QQ 及其他社交软件等）传递含有涉密信息、敏感信息的文件、资料。

7、 不得使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息。

8、 不得自行扩大涉密文件阅读范围。

9、 不得自行翻印、复印、摘抄、转载公开引用涉密文件。

10、未经审核，不得擅自对外公布、发送公司内部工作文件或敏感信息。

11、不得泄露、篡改、毁损收集的用户个人信息。

12、未经被收集者同意，不得向他人提供用户个人信息。

13、未经用户同意或者请求，或者用户明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。

14、不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动。

15、不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具。

16、明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

17、不得为无经营许可/备案的单位或者个人提供用于经营电信业务的电信资源或者提供网络接入、业务接入服务。

18、不得制作、复制、发布、传播含有以下违法违规内容的信息（“九不准”）：（1）反对宪法所确定的基本原则的；（2）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；（3）损害国家荣誉和利益的；（4）煽动民族仇恨、民族歧视，破坏民族团结的；（5）破坏国家宗教政策，宣扬邪教和封建迷信的；（6）散布谣言，扰乱社会秩序，破坏社会稳定的；（7）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；（8）侮辱或者诽谤他人，侵害他人合法权益的；（9）含有法律、行政法规禁止的其他内容的。

（三） 这些要知道

1、 **《关于印发中国电信用户个人信息管理办法（试行版）的通知》（中国电信〔2018〕328号）**

(1) 用户个人信息保护管理涵盖个人信息的收集、存储、使用、传输、销毁等各个环节中的相关行为，即在入网、办理、变更和销户等过程中所收集、存储、使用或销毁的纸质、光质、电磁质等载体承载的用户个人信息。

(2) 遵循合法、正当、必要、明确的原则收集、使用用户个人信息；按照“最小化够用”原则，只收集用户授权同意的与实现产品或服务功能有直接关联的个人信息类型和数量。

(3) 未经用户明示授权同意，不得收集、使用用户个人信息；不得违反法律、行政法规的规定和双方的约定收集、使用个人信息。

(4) 对查询、展示、导出和使用的用户个人信息，进行去标识化脱敏处理。

(5) 对于涉及到用户个人敏感信息的操作处理、批量数据导出等高风险系统管理操作，应当强制要求必须由 2 人或以上有相应权限的员工共同协作完成操作。

(6) 按最小授权原则，规范使用人角色的个人信息访问权限。

(7) 未经用户授权时（授权方式包括服务密码、证件号码、短信随机码、本机呼入、工单触发等），不得查询用户个人敏感信息。

(8) 对能接触到用户敏感个人信息的重点岗位实行监管、稽核，落实操作行为的日志记录、定期稽核与风险预警，防止用户个人敏感信息被非法查询、窃取、贩卖。

2、 **《关于印发<中国电信上海公司信息安全管理办法（2016 修订版）>的通知》（通用〔2016〕1 号）**

(1) 网络与信息安全工作坚持“谁管理谁负责，谁运营谁负责，谁使用谁负责”的原则。

(2) 新业务未经信息安全评估不得上线、发布或销售，评估范围涵盖自营业务、合作业务。

(3) 严格落实最终用户实名管理，加强对接入用户的身份审核和信息巡查。

(4) 与用户、合作方签订的纸质或电子协议中包含信息安全承诺书，明确对方需要遵守的信息安全相关要求，以及承担的信息安全责任。

(5) 对网络数据与网络信息的使用人员角色、认证信息、使用权限、访问控制策略等进行管理；对分配给使用人的认证信息进行备案，以便后续审计。

(6) 在对网络数据与网络信息进行操作与使用时，遵循既定访问控制策略，操作与使用涉及敏感数据或信息的，对操作对象进行脱敏。对使用者的访问记录、操作日志等信息进行留存，以便后续审计。

(7) 对于国际、国内标准或上级主管部门有明确要求的，需要进行完整性、保密性保护的重要网络数据与网络信息，采用加密传输，以防泄漏。

(8) 在网络或系统的规划、建设、运行时，严格落实网络信息安全“三同步”管理要求，做到网络信息安全管理要求与配套措施同步规划、同步建设、同步运行。

3、 **《关于印发<中国电信上海公司终端安全管理系统操作使用管理办法>的通知》（通用〔2016〕16 号）**

公司对接入企业内网的办公计算机终端进行安全准入控制，通过 TSM、堡垒机等措施，管控终端用户违反企业管理制度的行为。

（四）这些会受惩

1、 **《刑法》第二百五十三条之一【侵犯公民个人信息罪】** 违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

“情节严重”：（1）出售或者提供行踪轨迹信息，被他人用于犯罪的；（2）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；（3）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；（4）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；（5）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；（6）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；（7）违法所得五千元以上的；（8）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；（9）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；（10）其他情节严重的情形。

“情节特别严重”：（1）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；（2）造成重大经济损失或者恶劣社会影响的；（3）数量或者数额达到前款第三项至第八项规定标准十倍以上的；（4）其他情节特别严重的情形。

2、 **《刑法》第二百八十二条【非法获取国家秘密罪】** 以窃取、刺探、收买方法，非法获取国家秘密的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利；情节严重的，处三年以上七年以下有期徒刑。

【非法持有国家绝密、机密文件、资料、物品罪】 非法持有属于国家绝密、机密的文件、资料或者其他物品，拒不说明来源与用途的，处三年以下有期徒刑、拘役或者管制。

3、 **《刑法》第二百八十五条第二款【非法获取计算机信息系统数据、非法控制计算机信息系统罪】** 违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

单位犯罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

“情节严重”：（1）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；（2）获取第一项以外的身份认证信息五百组以上的；（3）非法控制计算机信息系统二十台以上的；（4）违法所得五千元以上或者造成经济损失一万元以上的；（5）其他情节严重的情形。

“情节特别严重”：（1）数量或者数额达到前款第一项至第四项规定标准五倍以上的；（2）其他情节特别严重的情形。

4、 **《刑法》第二百八十六条【破坏计算机信息系统罪】** 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

第一款和第二款规定的“后果严重”：（1）造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的；（2）对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的；（3）违法所得五千元以上或者造成经济损失一万元以上的；（4）造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；（5）造成其他严重后果的。

第一款和第二款规定的“后果特别严重”：（1）数量或者数额达到前款第一项至第三项规定标准五倍以上的；（2）造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；（3）破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序，致使生产、生活受到严重影响或者造成恶劣社会影响的；（4）造成其他特别严重后果的。

第三款规定的“后果严重”：（1）制作、提供、传输能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的程序，导致该程序通过网络、存储介质、文件等媒介传播的；（2）造成二十台以上计算机系统被植入能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的程序、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序的；（3）提供计算机病

毒等破坏性程序十人次以上的；（4）违法所得五千元以上或者造成经济损失一万元以上的；（5）造成其他严重后果的。

第三款规定的“后果特别严重”：（1）制作、提供、传输能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的程序，导致该程序通过网络、存储介质、文件等媒介传播，致使生产、生活受到严重影响或者造成恶劣社会影响的；（2）数量或者数额达到前款第二项至第四项规定标准五倍以上的；（3）造成其他特别严重后果的。

5、**《刑法》第二百八十六条之一【拒不履行信息网络安全管理义务罪】** 网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（1）致使违法信息大量传播的；（2）致使用户信息泄露，造成严重后果的；（3）致使刑事案件证据灭失，情节严重的；（4）有其他严重情节的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

6、**《刑法》第二百八十七条之一【非法利用信息网络罪】** 利用信息网络实施下列行为之一，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金：（1）设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；（2）发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；（3）为实施诈骗等违法犯罪活动发布信息的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

7、**《刑法》第二百八十七条之二【帮助信息网络犯罪活动罪】** 明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

8、**《网络安全法》第六十一条** 网络运营者未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

9、**《网络安全法》第六十三条** 从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等

帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

10、**《网络安全法》第六十四条** 网络运营者、网络产品或者服务的提供者侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

11、**《网络安全法》第六十六条** 关键信息基础设施的运营者在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

12、**《网络安全法》第六十八条** 网络运营者对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

13、**《网络安全法》第六十九条** 网络运营者有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：（1）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；（2）拒绝、阻碍有关部门依法实施的监督检查的；（3）拒不向公安机关、国家安全机关提供技术支持和协助的。

14、**《保守国家秘密法》第四十八条** 违反本法规定，有下列行为之一的，依法给予处分；构成犯罪的，依法追究刑事责任：（1）非法获取、持有国家秘密载体的；（2）买卖、转送或者私自销毁国家秘密载体的；（3）通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的；（4）邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的；

（5）非法复制、记录、存储国家秘密的；（6）在私人交往和通信中涉及国家秘密的；（7）在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密的；（8）将涉密计算机、涉密存储设备接入互联网及其他公共信息网络的；（9）在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换的；（10）使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息的；（11）擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；（12）将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途的。

有前款行为尚不构成犯罪，且不适用处分的人员，由保密行政管理部门督促其所在机关、单位予以处理。

15、**《保守国家秘密法》第四十九条** 机关、单位违反本法规定，发生重大泄密案件的，由有关机关、单位依法对直接负责的主管人员和其他直接责任人员给予处分；不适用处分的人员，由保密行政管理部门督促其主管部门予以处理。

机关、单位违反本法规定，对应当定密的事项不定密，或者对不应当定密的事项定密，造成严重后果的，由有关机关、单位依法对直接负责的主管人员和其他直接责任人员给予处分。

16、**《上海公司员工奖惩管理办法》第二十三条** 对于故意违反公司各项纪律、社会法纪的行为给予从重处理，即在不改变最终处分种类的情况下，适用比较高的处分。

17、**《上海公司员工奖惩管理办法》第二十九条** 员工凡有下列情形之一的，给予警告处分：（13）有证据证明是因个人管理不善被他人盗用仅限个人使用的公司内业务运营系统、通信网络系统或企业信息系统的账号密码,且盗用人已经按本办法或相关规定受到相应处理的。

18、**《上海公司员工奖惩管理办法》第三十条** 员工凡有下列情形之一的，给予记过处分：（7）将仅限个人使用的公司内业务运营系统、通信网络系统或企业信息系统的账号密码交由他人使用的。因该行为造成企业财产损失的，给予记大过处分。以此谋取私利，或给企业造成很大及以上财产损失或信誉损害的，或给客户造成损失的，解除劳动合同；（10）故意披露带有误导性、重大遗漏或者虚假的公司信息的、给企业造成财产损失或影响企业信誉的，给予记大过处分。以此谋取私利的，或给企业造成很大损失或给企业信誉造成极大损害的，解除劳动合同。

19、**《上海公司员工奖惩管理办法》第三十一条** 员工凡有下列情形之一的，给予记大过处分：（2）参与传播黄色、淫秽文字图片、出版物、照片、音像制品等物品的，如被公安部门查处的，解除劳动合同；（3）出于过失，将工作上获知的国家秘密、企业的商业秘密、商业机会或者客户信息，包括但不限于客户身份信息、联系方式、使用产品信息、通话记录、短信内容、影像录音等泄露给企业内外部，且基本没有损失或损失较小的；（6）利用工作便利，擅自变更涉及客户的各类资料数据，包括但不限于客户记费资料、客户属性、收据帐单、资费标准、收费项目等内容的。以此谋取私利的，或给企业、受害单位或个人造成财产损失的，或给企业信誉造成极大损害的，解除劳动合同；（10）盗用仅限他人个人使用的公司内业务运营系统、通信网络

系统或企业信息系统的账号密码的。以此谋取私利的，或给企业造成财产损失或信誉损害的，或给客户造成损失的，解除劳动合同；（13）超越工作职责范围或权限，侵入公司网络或信息系统，或者采用其他技术手段，获取公司网络或信息系统中存储、处理或者传输的数据，或者对该网络或信息系统实施非法控制，或者明知他人实施侵入、非法控制网络或信息系统的行为而为其提供便利，或对网络或信息系统功能进行删除、修改、增加、干扰，造成网络或信息系统非正常运行，有以上任一行为的。以此谋取私利的，或给企业、受害单位或个人造成财产损失的，或给企业信誉造成极大损害的，解除劳动合同。

20、**《上海公司员工奖惩管理办法》第三十二条** 员工凡有下列情形之一的，公司将作为违纪予以解除劳动合同：（6）采取不正当手段获取、披露、出卖国家秘密、企业的商业秘密、商业机会或者客户信息，包括但不限于客户身份信息、联系方式、使用产品信息、通话记录、短信内容、影像录音等，或者故意将工作上获知的国家秘密、企业的商业秘密、商业机会、客户信息泄露给企业内外部。或者虽非故意，但因泄漏以上信息，致使国家、企业遭受很大损失及以上的。

附：定义/术语

1、 **公民个人信息**：是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

2、 **用户个人敏感信息**：是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息，包括身份证件号码、住址、个人生物识别信息等。

3、 **关键信息基础设施**：是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施。

4、 **国家秘密**：是指关系到国家的安全和利益，依照法定程序确定的，在一定时间内只限一定范围的人员知悉的事项。分为绝密、机密、秘密三级。

5、 **商业秘密**：是指不为公众所知悉、能为企业带来经济利益、具有实用性并经企业采取保密措施的经营信息和技术信息。分为核心商业秘密、普通商业秘密两级。密级标注统一为“核心商密”、“普通商密”。

6、 **敏感信息**：指各类不涉及国家秘密或企业商业秘密的，若丢失、不当使用或未经批准被非限定人员获取、篡改、对企业造成不良后果的各类信息。

7、 **网络数据**：是指公司生产运营过程中收集、存储、传输、处理和产生的各种数据，主要包含业务运营数据，行业、公众用户信息，网络、平台以及上层应用的运行与维护数据等。

8、 **网络信息**：是指在公司网络（包括但不限于固网与移动网）接入、传送的视频、图片、文字、音频等公共信息内容。

附件 2

外包合作方员工信息统计表

上报单位/部门：

序号	姓名	手机