1. IT Environment & Evidence Guide

Local operating arrangement

ITG RESOURCES FZCO does not maintain any on-site servers or a dedicated server room at its UAE office. Employees access Group-provided internal systems over the network. Local server room inspection and maintenance records are therefore not applicable.

The attached workbench screenshot illustrates an internal application access interface. It does not establish the hosting location or architecture of the underlying systems. Those details remain subject to confirmation by Group IT.

Documents included

Pages 1-4: English overview and selected policy summaries for reviewer reference.

Pages 5-7: iGuoMao login guidance and account-access application procedures (Appendix A).

Page 8: Internal application workbench screenshot (Appendix B).

Pages 9-15: Seven supplied screenshots of the Group Information Security Management Regulations, in their original sequence (Appendix C).

Policy identification

Issuer: Xiamen ITG Group Corp., Ltd.
Document reference: Xia Guo Mao Ban [2025] No. 52.
Issue date: 7 April 2025.
Scope stated in Article 2: headquarters functions and directly controlled operating entities. The document is presented as the Group policy reference supporting the company's use of Group systems.

English sections are a working summary of selected provisions, not a certified or full translation. Original Chinese screenshots are retained for verification. Policy requirements are distinguished from evidence of actual implementation.

2. Account Access & Security Governance

Account access procedures

New employees: HR initiates the A401.3 (Automatic) IT Resource Provision Process. IT adds the account to the whitelist and provides an initial password. The employee then logs in using the assigned username and password. (Appendix A, pages 5-6)

Existing employees: Submit an A118 Application System Access Request through OA. Following IT processing, direct password login is enabled. (Appendix A, page 7)

English interface: A request may be submitted through MiaoXiaoXing; once approved, the simpler English interface becomes available. The notice describes direct password login without SMS verification to a Mainland China mobile number. (Appendix A, pages 5 and 7)

Selected Group policy provisions

Responsibilities - Articles 6-9: The Group establishes information security leadership and incident-response arrangements. The digital management department coordinates network management, information security systems, routine security work and incident response. Relevant operating entities carry out their assigned responsibilities. (Appendix C, pages 9-10)

Physical server room security - Article 20: Access approval and visitor registration are required; unauthorized personnel must not enter. External computers, storage devices and software require approval and inspection. Regular server room inspections and records are required. These are Group policy requirements; no local UAE server room is maintained. (Appendix C, page 11)

User accounts and endpoints - Articles 46-53: Restrictions cover unauthorized remote-access tools and network devices, personal account sharing, external-user account validity, unauthorized software, confidential files, email attachments and antivirus checks. (Appendix C, page 13)

3. Server, Backup & Recovery Controls

Selected English policy summary

Network security - Articles 29-35

The policy requires network monitoring, controlled access to security equipment, regular security inspections, software patching, configuration backups, antivirus protection and controlled remote access. Server operations are subject to auditing; audit logs are to be retained for at least 180 days. (Appendix C, page 12)

Applications and servers - Articles 36-38

Application systems are subject to security testing and account-access controls. Users are assigned differentiated permissions, and unauthorized access is prohibited. Production rollout requires security assessment, agreed maintenance responsibilities and appropriate testing before deployment. (Appendix C, page 12)

Data backup - Article 39

Security administrators are required to back up the data centre host systems, applications and data, and test restoration using backup media. Application owners must define backup arrangements. In principle, recovery should be possible to a point within the preceding month. Externally accessible websites and important internet-accessible hosts must have regular backups of system and application data and system images. Specific requirements are to be included in backup arrangements. (Appendix C, page 12)

Recovery safeguards - Article 40

A test environment and system recovery verification are required before system changes. Before system installation, administrators must create a complete host backup snapshot to support timely rollback if installation is unsuccessful. (Appendix C, pages 12-13)

Maintenance - Articles 41-45

The policy addresses server maintenance windows, physical security, antivirus protection, recording of operating-system and host-configuration changes, approved software updates, password management, routine inspection and verification of major changes. (Appendix C, page 13)

These clauses describe required controls. They do not establish the actual backup frequency, retention period, hosting location or restoration-test results of the particular systems used by ITG RESOURCES FZCO.

4. Audit Cross-reference & Evidence Status

Checklist item 26 - Internal server

The UAE office has no on-site server. Pages 1-3 describe the local arrangement and selected Group controls. Appendices A-B provide access guidance and an application workbench example; the latter is not a verified inventory of systems used by the UAE company.

Checklist item 27 - Server room and maintenance

No local server room is maintained. Group policy sets physical access, inspection and maintenance requirements. Actual Group hosting details and maintenance records are not held in this supporting pack.

Checklist item 32 - IT personnel and support arrangements

IT support is centrally coordinated by Xiamen ITG Group Corp., Ltd. Details of responsible IT personnel, competence, job descriptions and any outsourced support providers or contracts are managed at that level. ITG RESOURCES FZCO does not separately hold these materials.

Checklist item 33 - Networking system and service provider details

The UAE office internet service provider is du. Appendix E (pages 18-19) contains the supplied du account overview and profile screenshots. Internal IT coordination remains at Xiamen ITG Group Corp., Ltd. level; detailed Wi-Fi / LAN topology and configuration records are not included.

Checklist item 34 - IT hardware and software inventory

IT hardware and software inventory arrangements are centrally coordinated by Xiamen ITG Group Corp., Ltd. ITG RESOURCES FZCO does not separately hold the corresponding inventory records.

Related item 35 - Antivirus and firewall

The company uses Sangfor EDR for endpoint protection. Appendix D (pages 16-17) includes the internal deployment portal, an English introduction and a running client screenshot. The client shows a virus database update dated 3 November 2026 and 10 enabled real-time protection items. These screenshots do not constitute software licence or standalone network firewall evidence.

Checklist item 38 - Backup, restore and IT policy

Appendix C includes the Group policy; Articles 39-40 address backup and recovery. System-specific backup schedules, retention periods, backup success records and restoration-test records are not included.

Central coordination and evidence availability

IT support and inventory arrangements are coordinated by Xiamen ITG Group Corp., Ltd. The UAE office internet provider is separately identified as du, supported by Appendix E. Further technical and inventory records would need to be coordinated through the responsible teams.

Appendix A1 - iGuoMao Login Notice

Original screenshot retained. English guidance appears on pages 1-4.

【i国贸更新】Easier Login, Simpler English Interface

时间：2026-04-15　浏览：203　页面编辑：刘垚鑫　复核：杨闽

What’ s New in iGuoMao:

Easier Login, Simpler English Interface

Using iGuoMao overseas just got easier. To better support our overseas team and improve the experience for all users, iGuoMao now comes with two updates:**What’ s New**

- **No SMS verification required for login.**

You can now log in to iGuoMao without SMS verification sent to a Mainland China mobile number.

- **A simpler interface is now available.**

The new English interface is cleaner, easier to navigate, and built around the functions you use most.

How to Apply

01 **Apply for Direct Password Login**

For New Hires

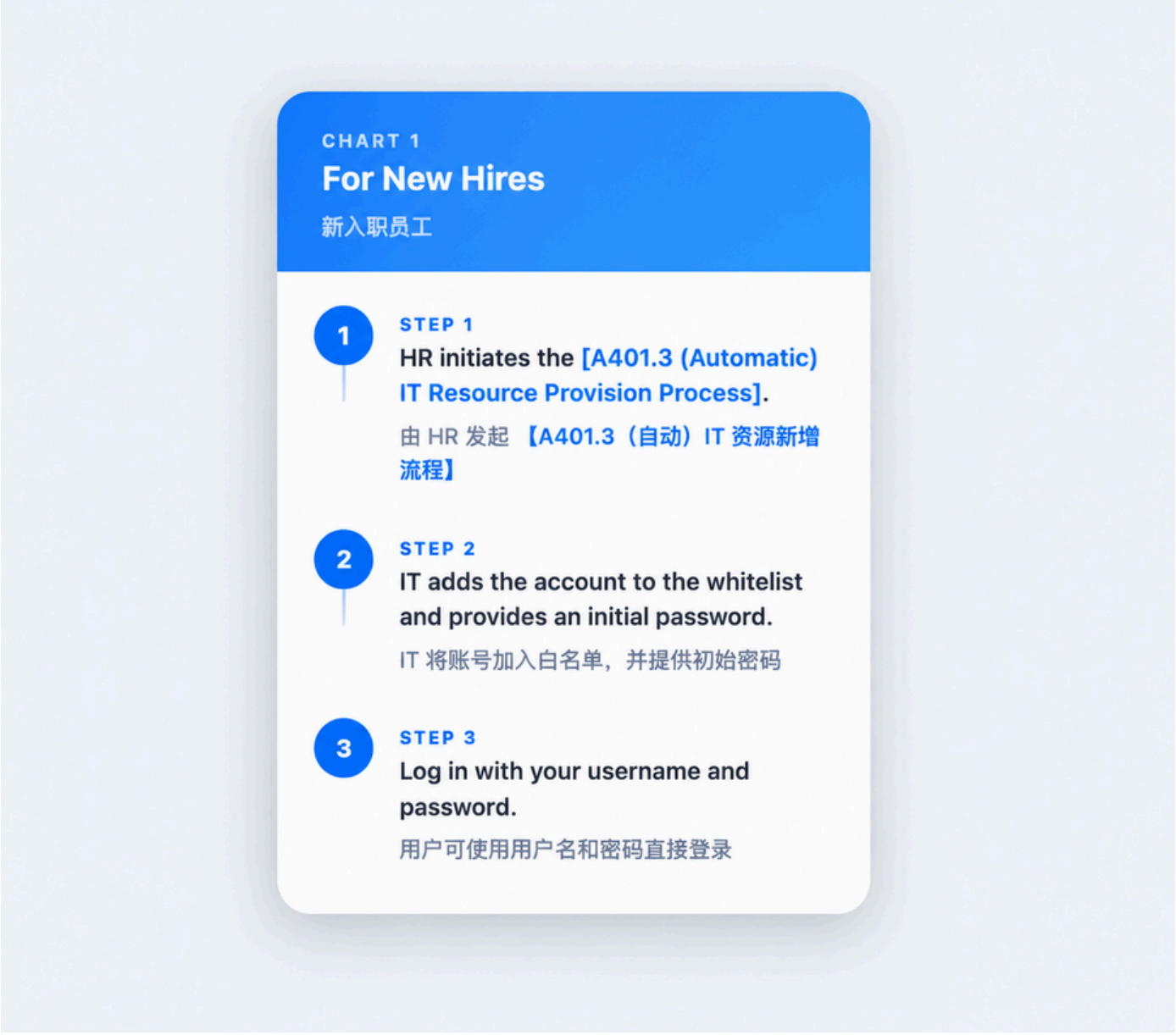
Step 1 - HR initiates the **[A401.3 (Automatic) IT Resource Provision Process]**.

Step 2 - IT adds the account to the whitelist and provides an initial password.

Step 3 - Log in with your username and password.

Appendix A2 - New Employee Access

Original screenshot retained. English guidance appears on pages 1-4.



Appendix A3 - Existing Employee Access

Original screenshot retained. English guidance appears on pages 1-4.

For Existing Employees

Step 1 - Submit an **[A118 – Application System Access Request]** via OA.

Step 2 - IT enables direct password login after processing your request.

Step 3 - Log in with your username and password.



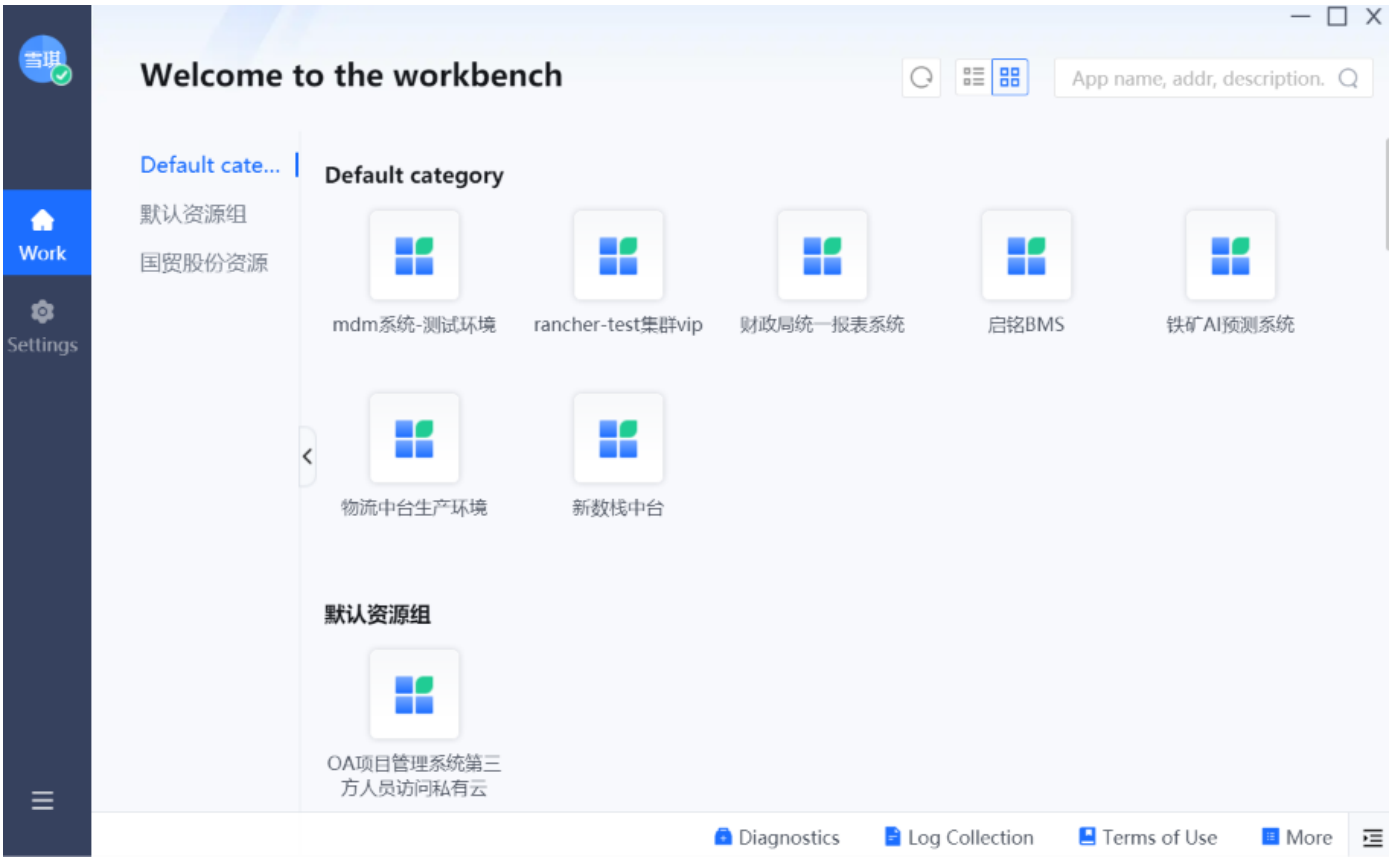
02 Apply for the Simpler English Interface

Step 1 - Submit a request via **MaoXiaoXing**.

Step 2 - Once approved, you can start using the simpler English interface in iGuoMao.

Appendix B - Application Workbench

Original screenshot retained. English guidance appears on pages 1-4.



Appendix C1 - Group Security Policy

Original screenshot retained. English guidance appears on pages 1-4.

信息安全管理规定

时间：2025-04-07　浏览：581　页面编辑：黄文谷　签标：杨闻

厦国贸办〔2025〕52号

厦门国贸集团股份有限公司

信息安全管理规定

第一章 总则

第一条 为保证厦门国贸集团股份有限公司数字化信息安全的安全、稳定，健全公司安全管理体系，加强公司数字化信息安全管理，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》和《网络数据安全管理条例》等法律关于信息安全管理的规定，结合公司实际情况，制定本规定。

第二条 本规定适用于厦门国贸集团股份有限公司（以下简称"公司"或"国贸股份"）本部各部门及其全资、控股（包括绝对控股和相对控股）、实际控制的各经营单位（以下简称各经营单位）。

第二章 定义

第三条 信息安全，指保护公司及各经营单位，通过信息系统、网络或服务器、客户端、移动端等以电子数据形式处理或存储的信息及信息系统免受未经授权的进入、使用、泄露、破坏、修改、检视、记录及销毁的行为。

第四条 重保，指在重大会议、节假日等重要敏感时期，对网络基础设施、重点网站和信息系统安全防护与安全保障，以确保公司网站、系统、数据安全平稳运行。

第五条 新媒体，指以公司或各经营单位名义开设、作为对外新闻发布渠道使用的自有新媒体账号，包括但不限于微信公众号、视频号、微博、抖音等。不包括与公司自有新媒体账号绑定、但不用于对外信息发布的媒介载体，如微信小程序、微信等。

第六条 新闻宣传，指在公司及各经营单位内外部网站、OA办公系统、APP、自有新媒体渠道、第三方报刊杂志、广播电视和互联网媒体等平台发布的，与公司品牌形象、业务内容相关的，除业务营销以外的文字、数据、图片、音像、链接以及其他形式的信息。

第三章 组织与职责

第七条 公司设立网络与信息安全领导小组，负责统一领导公司及各经营单位信息安全工作。网络与信息安全领导小组下设办公室，成员包括公司数字化部门的分管领导、公司总裁办公室负责人、公司品牌管理部负责人、公司数字化管理部负责人等，负责落实领导小组数字化信息安全管理工作，监督检查日常网络与信息安全工作，负责信息安全事故处置及责任认定。

第八条 公司设立信息安全事件应急领导小组及信息安全事件应急工作小组。信息安全事件应急领导小组负责公司信息安全事件应急处置组织、协调和领导工作，成员包括公司数字化部门的分管领导、公司数字化管理部负责人；信息安全事件应急工作小组负责公司信息安全事件的预防、监测、报告和应急处置工作，成员包括相关经营单位负责人、安全管理员、网络管理员、系统管理员等。

第九条 信息安全管理方主要职责：

（一）公司数字化管理部

1.根据公司数字化战略，统筹数字化信息安全项目建设需求，统筹规划网络信息安全策略；

2.负责公司网络安全管理，组织制定信息安全管理制度，组织开展日常信息安全工作，组织管理和维护网络安全设备与服务，监督检查公司及各经营单位信息安全工作；

3.对接网信部门、公安机关及上级单位等其他网络信息安全部门，组织协调处置信息安全事件。

（二）公司品牌管理部

1.负责国贸股份内外部新闻宣传管理；

2.负责统筹管理国贸股份新媒体矩阵。

（三）其他部门与各经营单位职责

Appendix C2 - Group Security Policy

Original screenshot retained. English guidance appears on pages 1-4.

1. 负责集团股份内外部新闻宣传管理；

2. 负责统筹管理国贸股份新媒体部门。

（三）其他部门与各经营单位职责

1. 遵守公司信息安全管理规定，积极配合公司网络信息安全工作；

2. 及时通报信息安全问题或事件。

第四章 网络规划管理

第十条 公司网络规划，包括且不限于引进新安全设备和安全服务、网络安全架构、公有云接入公司数据中心、境外平台接入公司内部网络等。数字化建设主办方或外部承办方提报方案后，由数字化管理部组织评审小组进行方案评审，依据评审通过的网络规划方案，组织人员进行建设实施，实现建设目标。对于境内异地平台接入公司内部网络，数字化管理部可直接组织人员建设实施。

第十一条 网络管理员负责对公司网络划分不同的安全区域，并按照方便管理和控制的原则为各网络区域分配IP地址，控制网络安全风险，降低系统风险。用户不得自行设置IP地址。

第十二条 网络信息安全相关的重大变更，包括可能会造成公司网络中断或业务中断的变更，由数字化建设主办方或外部承办方提交变更申请，说明变更原因、影响范围和实施方案，并经公司数字化管理部审批通过后执行。

第十三条 公司数字化管理部负责数据中心建设的统筹规划，禁止其他部门或各经营单位自建设数据中心、租用第三方数据中心或公有云。

第五章 互联网信息安全管理

第十四条 公司数字化管理部负责互联网应用安全管理。互联网应用，指开设互联网网站、API及新媒体上发布应用。

第十五条 涉及新媒体安全管理，遵照《厦门国贸集团股份有限公司新媒体管理办法》执行。涉及新闻宣传管理，遵照《厦门国贸集团股份有限公司新闻宣传管理办法》执行。

第十六条 公司及各经营单位互联网站开设、API及新媒体上发布应用，报公司数字化管理部组织测评及审核后，方可发布。开放互联网服务或应用的，须明确服务或应用的系统安全管理员及安全责任单位，安全责任单位的负责人为责任人。安全责任单位负责日常运维管理及风险事件监测，发生安全风险事件应第一时间处置。

第十七条 互联网服务接入基本要求：

（一）互联网发布的网站必须进行安全防护，应在信息系统内外网网络边界部署防火墙、审计系统、IPS等安全设备；

（二）互联网发布的网站必须使用网页防篡改技术或专用安全设备进行保护，确保网站在受到破坏时能自动恢复；

（三）互联网发布的网站必须经过安全测评才可上线，确保应用系统的安全性；

（四）互联网发布的网站应使用公司统一的域名后缀：tg.com.cn，如果需要注册或使用其它域名，应得到公司品牌管理部及数字化管理部的批准；

（五）需要进行网络安全等级保护的，由系统建设方负责申请备案，由安全管理员组织测评，系统建设方应配合提供材料与测评验证，积极修复测评过程中发现的问题；

（六）统一记录互联网服务URL清单台账，定期进行安全漏洞扫描，及时修复发现的中高危漏洞；

（七）重保防护。在重保期前，安全管理员梳理网络安全保障方案，明确保障目标、内容、方式、应急措施和人员值班表，向公司数字化管理部报备；在重保期间，系统安全管理员协调资源及时处置各类网络安全风险事件，接受公司网络与信息安全领导小组、办公室及公司数字化管理部的监督检查；在重保期后，系统安全管理员梳理网络安全重保工作报告，提交至公司数字化管理部报备。出现网络安全风险事件，第一时间报环处置。

第十八条 严禁用户利用公司网络或设备制作、复制、发布、传播下列有害信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）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；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

Appendix C3 - Group Security Policy

Original screenshot retained. English guidance appears on pages 1-4.

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会工公司稳定的；

（七）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

（八）公然侮辱他人或者捏造事实诽谤他人的；

（九）损害国家机关或公司信誉的；

（十）含有违反宪法和法律、行政法规及公司制度的。

第十九条 发现有害信息后，公司数字化管理部将采取隔离、断网等必要技术手段防止其扩散，责成责任单位及时处置。网情事件，遵照《厦门国贸集团股份有限公司网情应对管理办法》执行。

第六章 机房及数据安全管理

第二十条 数字化管理部负责公司机房管理，可以根据公司管理规范委托第三方进行，落实机房安全保障措施，包括且不限于：

（一）任何人员进入机房前须进行出入登记。无关人员不得进入机房，必要时须经数字化管理部批准，且由数字化管理部指定人员全程陪同；

（二）外协人员禁止携带笔记本电脑、相关存储设备及未经检查的软件介质等进入机房。若确需使用携带的笔记本电脑，应由数字化管理部指定人员进行检查和登记后方可携带进入机房使用；

（三）定期定时进行机房巡检工作，并填写巡检记录表。

第二十一条 公司数字化管理部监督检查数据安全管理措施，协调处理数据安全事件，组织数据安全应急演练。

第二十二条 任何个人和组织开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动：

（一）危害国家安全、荣誉和利益，泄露国家秘密和工作秘密；

（二）侵害他人名誉权、隐私权、著作权和其他合法权益等；

（三）通过窃取或者以其他非法方式获取数据；

（四）非法出售或者非法向他人提供数据；

（五）制作、发布、复制、传播违法信息；

（六）法律、行政法规禁止的其他行为。

任何个人和组织知道或者应当知道他人从事前款活动的，不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。

第二十三条 应用系统生产运行前，应明确备份、加密、访问控制等策略，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，应对数据安全事件，防范针对和利用数据的违法犯罪活动，维护数据的完整性、保密性、可用性。应用系统管理员对应用系统数据安全负责。

第二十四条 应用系统管理员应当建立数据安全应急处置机制，发生数据安全事件时及时启动应急响应机制，采取措施防止危害扩大，消除安全隐患。

第二十五条 禁止任何人未经审批私自持有、复制公司数据。因测试需要而使用真实数据，需经数字化管理部审核通过后，由数字化管理部指定人员协助应用系统开发人员完成数据的脱敏处置。

第二十六条 使用或建设SaaS服务模式的应用系统，需要将公司内部数据存储到第三方数据中心的，数字化建设主办方或外部承办方应和外部服务商沟通，提供系统安全证明和数据保密协议等材料，并经数字化管理部审核通过。

第二十七条 通过外包服务单位建设的应用系统，服务合同应包含数据保密协议，明确外包服务单位履行数据保密责任。定期根据外包服务协议中的安全要求，监视、评审由外包服务单位提供的服务、报告和记录，监督协议规定的信息安全条款和条件的严格执行。

第二十八条 员工在使用AI工具、博客和网盘等外部应用服务时，必须遵守公司规定与法律法规，严禁上传公司内部的涉密文件、敏感数据或其他保密信息。员工及各经营单位，应履行数据保密责任，不得恶意窃取、篡改、

Appendix C4 - Group Security Policy

Original screenshot retained. English guidance appears on pages 1-4.

申核通过后，由数字化管理部指定人员明确应用系统开发人员访问数据的权限范围。

第二十六条 使用或建设SaaS服务模式的应用系统，需要将公司内部数据存储到第三方数据中心的，数字化建设主办方或外部承办方应和外部服务商沟通，提供系统安全证明和数据保密协议等材料，并经数字化管理部审核通过。

第二十七条 通过外包服务单位建设的应用系统，服务合同应包含数据保密协议，明确外包服务单位履行数据保密责任。定期根据外包服务协议中的安全要求，监视、评审由外包服务单位提供的服务、报告和记录，监督协议规定的信息安全条款和条件的严格执行。

第二十八条 员工在使用ai工具、博客和网盘等外部应用服务时，必须遵守公司规定与法律法规，严禁上传公司内部的机密文件、敏感数据或其他保密信息。员工及各经营单位，应履行数据保密责任，不得恶意窃取、篡改、毁损、泄露公司数据。

第七章 网络信息安全

第二十九条 网络设备运行状况由网络管理员负责监控，包括机房所属的网络设备和办公区域出口网络设备。异地和境外平台的局域网网络设备及安全设备，由所在单位指定网络安全联络员配合公司数字化管理部指定人员进行管理，所在单位负责人为局域网络信息安全责任人。

第三十条 安全设备应限制在指定安全区域登录访问，账号采用强密码规则并定期修改。安全设备的运维操作应通过堡垒机审计，记录审计日志。

第三十一条 每季度对网络和安全设备进行安全巡检和漏洞扫描，对发现的安全漏洞进行及时的修补，根据厂家提供的软件升级版本对设备进行必要的更新。每季度对网络和安全设备配置进行离线备份，对于配置经常变更的设备应设置定期做一次离线备份，避免因设备故障导致重要配置丢失。

第三十二条 在网络各个边界部署防火墙等安全设备，并开启相应的防护策略。在网络关键节点处监视网络攻击行为，检测和阻断外部攻击以及内部发起的攻击。安全管理员负责定期排查安全防护设备、防火墙策略及安全日志进行检查，协调资源及时处置发现的安全风险事件，并持续优化公司网络安全防护体系。

第三十三条 制定网络安全应急预案，定期组织内部演练，或者积极参与外部网络安全演习，提高应急响应水平，落实应急响应保障措施。

第三十四条 服务器端口访问控制策略采用默认禁止和最小化原则的原则，即除非经过审批，许可，否则禁止所有的访问行为。访问控制策略的变更应经过申请和审批，并统一记录台账。对于已失效的访问控制策略，申请人应及时提申请删除，避免僵尸策略。

第三十五条 未经数字化管理部允许，应用系统管理员禁止在服务器上安装远程桌面工具。对服务器的维护操作只允许通过堡垒机进行访问，为满足安全审计要求，堡垒机审计日志应设置至少保存180天。生产环境数据库服务的运维操作应通过堡垒机审计，禁止将生产环境数据库和中间件服务端口直接暴露到办公网或VPN。原则上，不允许外部第三方人员直接登录访问应用系统生产环境的服务器和数据库。

第八章 应用及服务器信息安全

第三十六条 为避免安全风险并保障应用系统生产环境的稳定运行，应用系统生产环境、预生产环境和开发测试环境要分离，禁止共用同一套环境。

第三十七条 应用系统应包含权限控制模块，对不同的用户角色分配不同权限，禁止未授权访问。控制应用系统不同相关方角色的资源访问权限，原则上，不允许外部第三方人员直接登录访问应用系统生产环境和预生产环境的服务器和数据库资源。

第三十八条 应用系统生产环境正式上线运行前，须经过安全测评才能正式上线运行。由系统管理员填报《系统安全测评表》，安全管理员与应用系统管理员进行现场访谈，双方协商后确定测评内容和测评时间。原则上，系统安全测评需经漏洞扫描、渗透测试，验证系统不存在高、中危的安全漏洞。应用系统管理员根据系统架构复杂度并展系统上线前的应急演练，并在演练前提交《演练方案》，在演练结束后提交《演练报告》。应用系统管理员应提供服务器开关机顺序，并与服务器管理员确认重要数据的备份方式及备份策略。

第三十九条 安全管理员每季度对数据中心所有主机进行漏洞扫描，并将扫描出漏洞中，高危漏洞分类整理后，通知相关的应用系统管理员处理。原则上，应用系统管理员应在一个月内修复高危漏洞，三个月内完成所有漏洞修复。互联网站点及从互联网可直接访问到的主机，其高、中危漏洞都必须全部修复。公司数字化管理部定期检查安全漏洞扫描及修复情况。

第四十条 修复安全漏洞之前，应用系统管理员应建立测试环境检验修复效果，确认无异常后方可在生产系统安装补丁，在生产系统安装补丁之前通知服务器管理员创建生产主机的“备份快照”以便在补丁修复不成功时可快速回滚恢复。

Appendix C5 - Group Security Policy

Original screenshot retained. English guidance appears on pages 1-4.

第四十条 修复安全漏洞之前，应用系统管理员应建立测试环境检验修复效果，确认无异常后方可在生产系统安装补丁，在生产系统安装补丁之前确和服务器管理员创建生产主机的“备份快照”以便在补丁修复不成功时可快速回滚恢复。

第四十一条 对于尚无官方补丁的安全漏洞，漏洞修复责任人可在说明原因后暂缓修复，待相应补丁公布后尽快修复；对于升级补丁可能导致系统异常的安全漏洞，在提供充分的证明材料后也可暂缓修复。因上述两种情形暂时没有修复的安全漏洞，服务器管理员应尽可能通过虚拟补丁系统进行临时封堵。

第四十二条 服务器必须部署主机终端安全防护软件，用于病毒每入侵防护，并设置定期升级病毒库。开发人员如需临时关闭上述安全软件，应提前告知服务器管理员和安全管理员，并在事后及时恢复启用。

第四十三条 开发人员如需开启或关闭服务器上的主机防火墙或修改主机防火墙配置，应先报服务器管理员和安全管理员申请报备。

第四十四条 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级等方式保持系统补丁及时得到更新。操作系统用户密码应采用强密码规则并定期修改。

第四十五条 服务器管理员负责服务器备份策略管理，并定期进行备份。应用系统管理员应主动向服务器管理员提出备份的内容并根据实际情况和重要程度制定备份方式和策略，如出现变更应及时通知服务器管理员。应用系统管理员在对操作系统上的程序或配置执行重大的变更操作前，应先和服务器管理员确认并进行备份，避免变更出现故障时无法及时恢复。

第九章 客户端信息安全

第四十六条 员工不得将台式电脑随意搬离原放置场所，不得随意打开机箱，拆卸、更换电脑配件。电脑硬件变更或网络设备的搬迁，必须由桌面运维专员现场处理或授权处理。

第四十七条 电子设备，包括台式电脑、笔记本电脑、平板设备、手机等，首次接入公司网络需要使用域账号进行网络认证后才能访问公司内部网络资源。访客电子设备允许接入无线AP的访客频道访问互联网上的资源，但不能访问公司内部信息资源。

第四十八条 用户应使用各自的域账号登录公司内部网络，个人域账号实名申请，所有者应妥善保管自己的账号及密码信息，严禁将个人域账号交由他人使用。新入职员工通过入职流程申请域账号，员工离职后，删除已申请的域账号。

第四十九条 外部人员由用人单位通过OA流程代为申请临时域账号，临时域账号原则上有效期为90天，超期需要继续使用的，应办理临时域账号延期申请，外部人员域账号管理责任人为用人单位申请人。

第五十条 禁止用户私自在公司配置的电脑上安装未经授权的软件，包括可能对公司网络应用和安全造成严重影响的软件，如：嗅探工具、P2P类下载、挖矿软件等；禁止用户利用公司的网络资源散布淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪等内容，或法律法规禁止的其他内容的信息，禁止用户在上班时间玩电脑游戏、观看影视剧等影响办公场所秩序的行为。

第五十一条 员工如果长时间离开座位，应锁定电脑或将电脑关机，以免无关人员调阅电脑中的资料。员工的重要文档必须加密保存，员工的涉密电子文档不准通过共享文件夹传递，必须加密后通过可移动介质或电子邮件传递，密钥须通过其它方式传递给收件人，密钥应不少于8位字符。

第五十二条 员工对外收发邮件应统一采用公司提供的电子邮箱，以体现公司的企业形象和方便对邮箱进行统一的垃圾邮件和钓鱼邮件监测。员工使用邮件的基本安全要求：

（一）不要轻信发件人显示的“名称”，不放松对“熟人”邮件的警惕；

（二）不点击未经核实来源的邮件内的任何链接或附件内容，点开不明的邮件附件前记得先用杀毒软件扫描；

（三）不回复未经核实的邮件，对于来历不明、疑似钓鱼或诈骗的邮件，如：要求输入账号密码、验证码或扫描二维码等，员工应仔细辨别，必要时应与发件人再确认；

（四）邮箱密码应符合强密码规则并定期修改，严禁将邮箱账号交由他人使用。

第五十三条 员工的办公电脑必须安装公司指定的终端杀毒软件，并定期进行杀毒。对于病毒的防范，以预防为主，查杀为辅。员工要同步关注国际网络信息安全公众号或内部网站的安全提示信息，不断增强安全意识。

第十章 信息安全事件管理

第五十四条 信息安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患等因素，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济或公司造成负面影响的事件。包括：恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、违规操作事件、安全隐患事件、异常行为事件及其他事件。表现

Appendix C6 - Group Security Policy

Original screenshot retained. English guidance appears on pages 1-4.

（四）邮箱密码应符合强密码规则并定期修改，严禁将邮箱账号交由他人使用。

第五十三条 员工的办公电脑必须安装公司指定的终端杀毒软件，并定期进行杀毒。对于病毒的防范，以预防为主，查杀为辅。员工要同步关注国际网络信息安全公众号或内部网站的安全提示信息，不断增强安全意识。

第十章 信息安全事件管理

第五十四条 信息安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患等因素，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济或公司造成负面影响的事件。包括：恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、违规操作事件、安全隐患事件、异常行为事件及其他事件。表现为：蓄意制造、传播有害程序，或因受到有害程序的影响导致的信息安全事件；或公司网络遭受外部网络攻击；或公司内部生产数据被篡改、假冒、泄漏、窃取或删除；传播危害国家安全、社会稳定、公共安全和利益的有害信息；或人为使用非技术手段造成系统被损的；或发生钓鱼及诈骗邮件事件；或被网信部门和公安机关等网络安全主管部门通报的信息安全事件等。

信息安全事件按影响程度分为P0级，P1级和P2级三个等级，分级标准为：

（一）P0级别，最高级别事件，指导致特别严重影响或被损的信息安全事件。认定标准为：对外提供服务的应用系统，其页面被篡改为反动信息、煽动性信息或法律法规禁止的其他信息，造成严重政治影响的；或被网信部门和公安机关等网络安全主管部门通报的造成严重政治影响或特别严重经济和社会影响的信息安全事件。

（二）P1级别，严重事件，指导致严重影响或被损的信息安全事件。认定标准为：对外提供服务的应用系统其页面被篡改或恶意利用，发布虚假或诈骗等信息并已造成经济和社会影响；或蓄意制造、传播有害程序；或公司网络因遭受外部网络攻击，造成网络中断、瘫痪或数据被篡改、假冒、泄漏、窃取或删除；或违规操作造成公司业务损失或社会危害；或被网信部门和公安机关等网络安全主管部门通报的猖獗漏洞、钓鱼及诈骗邮件、病毒木马、违规情况等信息安全事件。

（三）P2级别，紧急事件，指导致较大范围影响或被损的信息安全事件。认定标准为：公司内部设备感染计算机病毒、蠕虫、木马、僵尸网络等有害文件；公司网络遭受大规模的拒绝服务攻击、后门攻击、漏洞攻击等网络攻击事件，但未造成网络中断或数据损失的；或违规操作未造成公司业务损失或社会危害；或公司内部登录凭证信息泄露，发生钓鱼及诈骗邮件事件；或其他不能归为P0和P1级别的信息安全事件。

其中，信息安全事件为P2级别以上的认定为信息安全事故。

第五十五条 判定为P0级事件的，应急工作小组组长应即刻向应急领导小组汇报。由应急领导小组组长指示下达应急预案启动指令，同时即刻组织协调应急工作小组开展应急处置工作。其中，涉及政治类重大影响事件的，由公司党委统一组织协调，应按相关要求立即上报上级公司党委、本单位党委、数字化管理部、网信部门和公安机关等网络安全主管部门。

第五十六条 判定为P1级和P2级事件的，由应急领导小组组长或副组长指示下达应急预案启动指令，迅速组织协调应急工作小组开展应急处置工作。

第五十七条 应急工作小组负责对事件进行研究分析和调查处理，查明网络安全事件的起因、性质、经过、影响和责任，提出调查处理建议和今后同类事件的安全防范措施，以防止同类事件再次发生。

第五十八条 当出现信息安全事故时，应急工作小组在事故发生后2日内出具事故现象描述文件，描述事故发生时间，事故现象，影响时长，影响范围，事故截图，应急处理措施；事故发生后7日内出具《事故分析报告》，说明事故原因，解决方案，预防措施。事故现象描述是《事故分析报告》的内容，可独立提交或合并在《事故分析报告》文件中，在事故发生后2日内一并提交。向公司数字化管理部报备。各经营单位应明确事故处置管理要求，督促信息安全事故及时妥善处理。

第五十九条 对下列情况可以经领导小组评估审核，报领导小组批准后予以奖励：在应急行动中做出特殊贡献的先进单位和集体；在应急行动中提出重要建议方案，节约大量应急资源或避免重大损失的人员；在应急行动第一线做出重大成绩的现场作业人员。

第六十条 对不按照规定制定预案和组织开展演练、迟报、谎报、瞒报和漏报信息安全事件重要情况或者信息安全事件应急管理工作中有其他失职、渎职行为的，对有关责任人予以通报批评并扣减绩效。情节严重的，处以行政处分；涉及犯罪行为的，由公安机关和司法机关依法追究刑事责任。

第十一章 信息安全宣传

第六十一条 针对发生的网络安全风险事件，公司数字化管理部应及时在公司内网消息渠道发布网络安全风险提醒通知，如：钓鱼诈骗邮件、病毒文件传播等。

Appendix C7 - Group Security Policy

Original screenshot retained. English guidance appears on pages 1-4.

第六十条 对不按照规定制定预案和组织开展演练，迟报、谎报、漏报和瞒报信息安全事件重要情况或者信息安全事件应急管理工作中有其他失职、渎职行为的，对有关责任人予以通报批评并扣减绩效。情节严重的，处以行政处分；涉及犯罪行为的，由公安机关和司法机关依法追究刑事责任。

第十一章 信息安全宣传

第六十一条 针对发生的网络安全风险事件，公司数字化管理部应及时在公司内网消息渠道发布网络安全风险提醒通知，如：钓鱼诈骗邮件、病毒文件传播等。

第六十二条 每年定期组织各种形式的安全意识教育活动，包括但不限于开展网络安全宣传周活动或开展网络安全意识培训、参加外部网络安全培训、网络钓鱼演练、安全材料宣传等，提升公司全员信息安全意识。

第十二章 附则

第六十三条 本规定经公司总裁办公会批准后生效。本规定自公布之日起执行。原厦国贸办〔2024〕128号《信息安全管理规定》及厦国贸办〔2021〕174号《信息技术管理规定》同时废止。

第六十四条 本规定授权公司数字化管理部负责解释。

厦门国贸集团股份有限公司

2025年4月7日

厦门国贸集团股份有限公司　　2025年4月7日印发

Appendix D1 - Endpoint Protection

Sangfor EDR (Endpoint Detection and Response)

Endpoint Protection Center

The company identifies Sangfor EDR as the endpoint security software used within its corporate network. It provides antivirus and endpoint protection functions. The internal portal below provides installation options for Windows, macOS and Linux endpoints.

Deployment notice - English translation

To strengthen endpoint security, Sangfor EDR Endpoint Protection Center is being deployed across endpoints. Please select the installation method appropriate to your operating system. No further configuration is required after installation. Thank you for your support and cooperation.

The portal instructions state that the endpoint agent connects automatically to EDR following successful installation. This screenshot documents the internal deployment arrangement; it does not establish installation status on every device.



Appendix D2 - Endpoint Security Status

Client interface - English explanation

The supplied client screenshot displays the following status for the pictured endpoint:

Virus database last updated: 3 November 2026.

Protection duration displayed: 88 days.

Today: no scan performed; no risk reported by the interface.

Real-time protection: 10 protection items enabled.

Blocking activity: zero blocked behaviours in the past 30 days.

The navigation includes Security Center, Virus Scan, Vulnerability Protection, Real-time Protection and System Tools. Visible functions include real-time file protection, ransomware protection, suspicious-software scanning and protection, and advertising pop-up blocking.



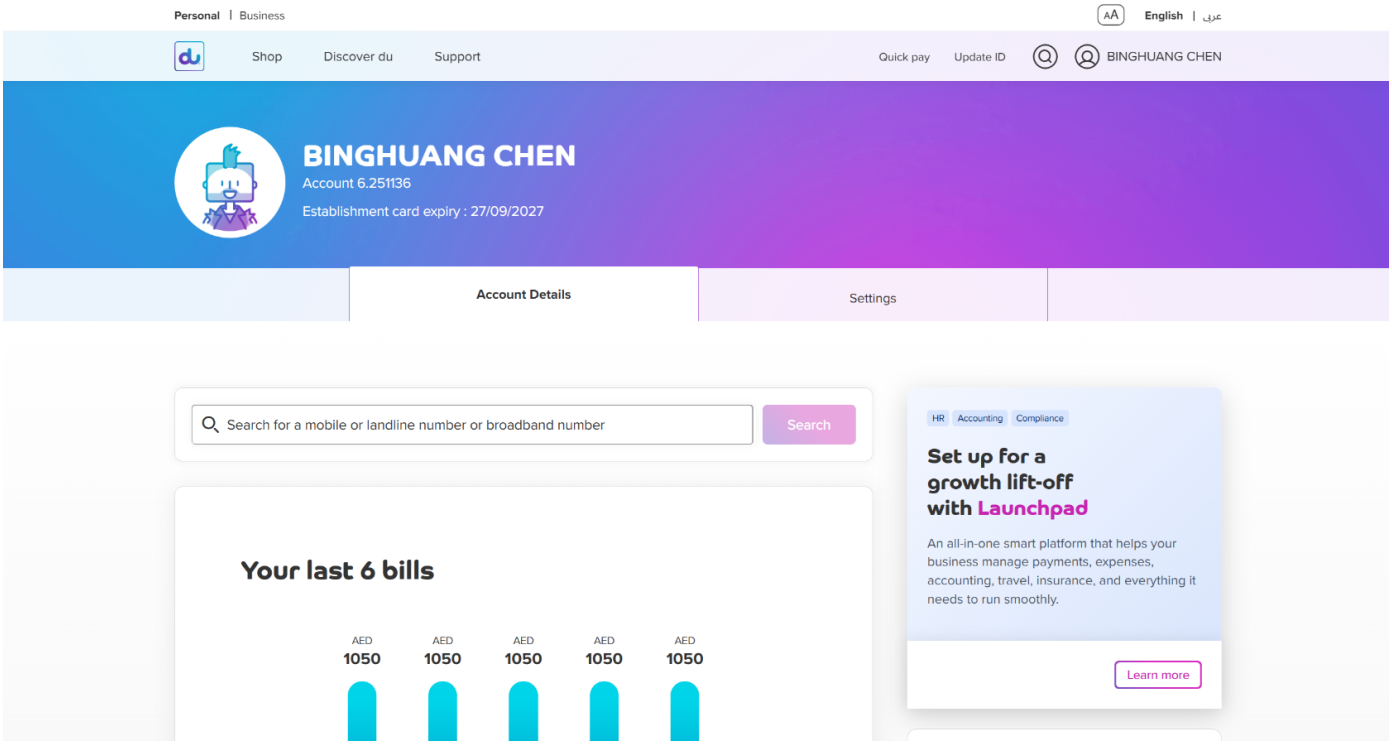
Evidence scope: this is a status snapshot of the pictured endpoint. It supports the presence of an operating endpoint protection client; it does not demonstrate fleet-wide coverage, software licensing or a separate network firewall configuration.

Appendix E1 - Office Internet Provider

Internet service provider: du

The company confirms that du provides internet connectivity for its UAE office. The supplied du account portal screenshot is included below as supporting evidence for checklist item 33 - Networking system and service provider details.

The portal displays account number 6.251136 and the account profile name BINGHUANG CHEN. These details are reproduced as displayed in the service provider portal.



Appendix E2 - Service Account Profile

du account profile and company reference

The supplied profile screenshot shows the company registration number DMCC902147 and the company contact email wuqianqian@itg.com.cn. It supplements the account overview on the preceding page.

The screenshots identify the service provider and account profile. They do not specify the office Wi-Fi / LAN topology, equipment configuration, connection speed or service contract terms.

