1. Project Charter — *EasyBusy Cybersecurity Design Project*

---

1. Company Overview

EasyBusy is a mid-sized e-commerce company with **50 employees**, operating from a **headquarters**, one **branch office**, and with **20% remote staff**. The company sells household goods online. It uses a **cloud-first model** — all key services are SaaS-based (email, CRM, accounting, and e-commerce platform).

Department	Main Functions	Total Staff	Location (HQ / Branch / Remote)	Notes
Management & HR	Strategic management, oversight, recruitment, compliance	6	4 HQ + 2 Remote	Includes CEO, HR manager, compliance officer
IT & Security	Network, endpoint, and SaaS administration; VPN; backups	8	6 HQ + 2 Remote	Responsible for technical systems, SaaS access, endpoint protection
Sales & Marketing	Customer engagement, promotions, advertising, campaigns	12	9 HQ + 3 Remote	Uses CRM for campaigns and analytics
Customer Support	Handling client inquiries, tickets, and complaints	8	6 HQ + 2 Remote	Uses CRM ticketing system
Finance & Accounting	Payments, invoices, accounting	6	5 HQ + 1 Remote	Manages accounts and financial records
Operations & Logistics	Warehouse, shipping, inventory management	10	5 HQ + 5 Branch	Branch office handles on-site logistics
Total		**50**	**40 on-site (35 HQ + 5 Branch) + 10 Remote**	—

EasyBusy stores **customer PII and order data** in SaaS systems; payments are processed via a **secure hosted checkout** (no card data stored locally).

---

2. Project Purpose and Scope

The project aims to design a **small business cybersecurity framework** for EasyBusy, aligned with:

- **CIS Controls v8 (Implementation Group 1)**
- **NIST Cybersecurity Framework (CSF)** — Identify, Protect, Detect, Respond, Recover

Objectives:

- Achieve **100% MFA coverage** across all systems.
- Ensure **endpoint protection** (EDR, encryption, patching) for all devices.
- Secure **VPN access** for remote users.
- Define clear **incident reporting** and **employee behavior rules**.
- Implement **SIEM monitoring**, **backup strategy**, and **least privilege access model**.

---

3. Team Roles and Responsibilities (See ANNEX 1 of the Project Charter for Details)

Person	Primary Role	Secondary Role	Responsibilities
Anahit **Project Manager (PM)**	Project lead	IR communications	Coordinates project scope, budget, and milestones; maintains Charter, RAID & ADR logs; oversees MFA and endpoint enforcement; ensures stakeholder communication.
Nerses **Lead Architect**	QA & Validation	—	Designs system and network topology; defines control matrix; validates SaaS compliance with security architecture and backup solutions.
Garegin **Identity & SaaS Engineer**	Compliance evidence	—	Implements IdP/SSO/MFA; manages user privileges (least privilege model); maintains SaaS configurations; collects access control evidence.
Harut **Network & Data Protection Engineer**	IR support	—	Configures VPN/Zero Trust model; defines endpoint policies by department; enforces encryption, patching, and backups (immutability).
Karine	Risk oversight	—	Deploys SIEM/MDR; manages alerts and triage; maintains metrics

Person	Primary Role	Secondary Role	Responsibilities
Security Operations Lead			(MFA %, phishing test results); trains staff on email security.
Yelena **Incident Response Lead & Documentation Officer**	Operations communications	—	Develops IR playbooks; coordinates tabletop exercises; updates policy documentation; ensures CIS/NIST mapping compliance.

---

4. Employee Cybersecurity Rules*

All employees must comply with EasyBusy's security policy:

1. **100% MFA** required for all systems (email, CRM, VPN).
2. **Endpoints** must have encryption, EDR, and automatic patching.
3. **Suspicious emails:** do not click or reply; report to security@easybusy.am.
4. **Access control:** only required privileges per role.
5. **Remote work:** VPN mandatory; use company-managed devices only.
6. **Data sharing:** use approved SaaS tools only; never share credentials.
7. **Incident reporting:** report anomalies immediately to Security Operations.
8. **Lost device:** report ASAP; IT will lock or wipe remotely.
9. **Quarterly training** mandatory for all departments.

***See ANNEX 2 of the Charter for the Detailed Rule List.**

---

5. Key Metrics (KPIs)

Metric	Baseline	Target	Frequency	Owner
MFA coverage	60%	100%	Monthly	Garegin
Endpoint encryption	70%	100%	Quarterly	Harut
Phishing simulation click rate	15%	<5%	Quarterly	Karine
Backup test success rate	80%	100%	Monthly	Harut
Incident response time	6 hrs	<2 hrs	Monthly	Yelena
VPN uptime	98%	>99.5%	Weekly	Harut

---

6. Incident Response (IR) Lifecycle Timeline

Phase	Description / Key Actions	Responsible Roles	Target Duration	Deliverables / Outputs
1. Preparation	- Maintain IR plan, playbooks, and contact lists. - Conduct awareness training and tabletop exercises. - Ensure SIEM alerts and monitoring baselines are configured. - Verify incident communication channels (email, Teams, phone).	PM, IR Lead, SecOps (Anahit, Yelena, Karine)	Ongoing (continuous)	Updated IR documentation, trained staff, baseline SIEM metrics
2. Detection & Analysis	- Identify suspicious activity via SIEM, endpoint, or user report. - Classify severity (Low / Medium / High / Critical). - Correlate alerts and validate incident scope. - Notify PM and management if High/Critical.	SecOps, IR Lead (Karine, Yelena)	**0–1 hour** from alert	Incident ticket created, alert verified, preliminary analysis
3. Containment (Short-term)	- Isolate affected systems (network or endpoint). - Disable compromised accounts. - Preserve forensic data and logs. - Communicate internally per IR plan.	IR Lead, Network Eng. , Identity Eng. (Yelena, Harut, Garegin)	**1–2 hours**	Containment confirmation, system isolation report
4. Eradication	- Identify root cause (malware, phishing, misconfig, insider). - Remove malicious code, revoke credentials, patch vulnerabilities. - Validate through follow-up scans and tests.	Network Eng. Lead Architect, IR Lead (Harut, Nerses, Yelena)	**2–6 hours**	Root cause analysis, remediation checklist
5. Recovery	- Restore systems from verified clean backups. - Reconnect to the	Data Protection Monitoring, Oversight	**6–24 hours**	System restoration

Phase	Description / Key Actions	Responsible Roles	Target Duration	Deliverables / Outputs
	production network. - Monitor for residual activity for 24–48 hrs. - Validate full service functionality.	(Harut, Karine, Anahit)		report, recovery validation log
6. Post-Incident Review (Lessons Learned)	- Conduct debrief with all involved teams. - Document timeline, impact, and response metrics. - Update IR plan and security controls accordingly. - Report findings to management.	PM, IR Lead, SecOps (Anahit, Yelena, Karine)	**Within 72 hours post-incident**	Post-incident report, updated playbook, KPI comparison

7. Governance and Communication

- Weekly progress sync between team members.
- PM provides biweekly updates to EasyBusy management.
- Critical incidents reported directly to Security Operations & IR leads.
- Project documentation maintained in shared repository (SharePoint).

---

8. Constraints and Assumptions

- CapEx ≤ $20,000
- OpEx ≤ $1,500/month (licenses & services)
- 50 employees, 60 total devices (PCs/laptops/phones)
- Limited IT staff — preference for managed security services
- SaaS-first infrastructure (no local servers)

Annex 1 to the Project Charter

Team Roles and Responsibilities

The cybersecurity project team consists of six members. Each member has a **primary** and **secondary** role, as well as clearly defined **responsibilities and deliverables** aligned with project goals under the NIST CSF framework (Identify, Protect, Detect, Respond, Recover).

Person	Primary Role	Secondary Role	Responsibilities & Key Outputs
Anahit – Project Manager (PM)	PM	Incident Response Communications	• Develop and maintain the **Project Charter**, **Plan**, **RAID** (Risks, Assumptions, Issues, Decisions), and **ADR** (Alternative Dispute Resolutions) logs. • Oversee project schedule, budget, and team coordination. • Maintain communication with company management and stakeholders. • Approve access policies, MFA enforcement, and endpoint management rules. • Conduct periodic stakeholder updates and ensure documentation compliance.
Nerses **Lead Architect**	Quality Assurance & Validation	• Design the overall **system security architecture** integrating SaaS, VPN, and branch topology. • Create **network segmentation diagrams** and control matrices. • Ensure SaaS platforms (email, CRM, accounting, e-commerce) are compliant with MFA and data protection standards.	

Person	Primary Role	Secondary Role	Responsibilities & Key Outputs
		• Review and validate implementation steps and maintain configuration baselines.	
Garegin **Identity & SaaS Engineer**	Compliance Evidence Collection	• Implement and manage **Identity Provider (IdP)**, **SSO**, and **MFA** for all users (100% coverage). • Manage user roles and permissions following **least privilege principle**. • Maintain SaaS configurations (email, CRM, file sharing, accounting). • Provide compliance evidence for identity and access controls.	
Harut **Network & Data Protection Engineer**	Incident Response Support	• Design and maintain **VPN/Zero Trust architecture** for secure remote access. • Define **endpoint protection standards** for each department (antivirus, encryption, patch management). • Implement **backup strategy** (immutability, recovery testing). • Define **RPO/RTO** metrics and ensure operational resilience.	
Karine **Security Operations Lead**	Project Risk Oversight	• Set up **SIEM/MDR** integration for centralized log collection and alert management. • Create **incident triage** and **runbooks** for early threat detection. • Monitor system metrics and assess risks related to user behavior (e.g.,	

Person	Primary Role	Secondary Role	Responsibilities & Key Outputs
		phishing). • Train staff on how to handle suspicious emails and escalate incidents.	
Yelena **Incident Response Lead & Documentation Officer**	Operations Communications	• Develop and maintain **Incident Response (IR) plans and playbooks**. • Conduct tabletop exercises and ensure staff readiness. • Prepare **policy pack** aligned with **CIS/NIST** frameworks. • Coordinate response communication during security incidents. • Document all procedures and maintain compliance mapping.	

Annex 2 to the Project Charter

Employee Cybersecurity Rules and Guidelines

These policies apply to **all EasyBusy employees** (onsite, branch, and remote). Every employee must understand and follow these cybersecurity rules to protect company data, systems, and customers.

---

1. Phishing and Suspicious Emails

If you receive an unusual or suspicious email:

- **Do not click** on links or open attachments.
- **Do not reply** to the sender.
- Report it immediately to **Security Operations (security@easybusy.am)**.
- Wait for confirmation before deleting or taking any further action.
- If you accidentally clicked a link, **disconnect your device from the network** and contact IT support immediately.

---

2. Passwords and Authentication

- Use **Multi-Factor Authentication (MFA)** for **all** systems (email, CRM, SaaS, VPN).
- Passwords must be **unique, at least 12 characters**, and contain letters, numbers, and symbols.
- **Never reuse passwords** across systems.
- Change your password immediately if you suspect compromise.
- **Do not share** your password with anyone — not even IT staff.

---

3. Lost or Stolen Device

If your laptop or phone is lost or stolen:

- Notify **IT Security (helpdesk@easybusy.am) IMMEDIATELY**.
- Provide details: last known location, device type, and owner.
- The IT team will remotely lock or wipe the device if needed.
- Never store unencrypted data on USB drives or personal devices.

4. Working Remotely

- Always connect via the **company VPN** with MFA.
- Do not use public Wi-Fi without a VPN.
- Keep your screen locked when away from your computer.
- Ensure your device runs **endpoint protection software** (EDR, antivirus, encryption).
- Save files only on approved **cloud storage (OneDrive/SharePoint)**, not on local disks.

---

5. Handling Sensitive Data

- Treat all customer information and financial data as **confidential**.
- Do not copy or download databases unless explicitly authorized.
- Share data only through secure, approved platforms (not via email attachments).
- Verify recipients before sharing files.
- Use **"Need-to-know" principle** — access only data required for your work.

---

6. Reporting Incidents

If you notice unusual activity such as:

- Unexpected system slowdown
- Unknown logins or login alerts
- Missing or changed files

→ **Immediately report** to Security Operations with time, system, and user details.
Early reporting can prevent wider damage.

---

7. Software and Updates

- Install software **only from approved sources** (IT-managed installations).
- Do not install personal or unverified apps.
- Restart your computer regularly to apply security patches.
- Ensure antivirus and system updates are always **enabled and current**.

---

8. Use of External Media

- Do not plug in unknown USB drives or external disks.
- If external media is required, use **encrypted, company-approved** devices.
- Scan all external devices with antivirus before use.

---

9. Social Engineering Awareness

- Be cautious with **unexpected phone calls, texts, or chats** asking for credentials or payments.
- Always verify the identity of the caller through official channels.
- Do not share sensitive information via messenger apps or SMS.

---

10. After an Incident

- Follow the instructions from the **Incident Response (IR) team**.
- Do not attempt to fix or delete evidence yourself.
- Cooperate fully with investigation steps and provide requested information.
- Participate in post-incident awareness sessions if invited.

---

11. Periodic Training

- All employees must complete **quarterly cybersecurity awareness training**.
- Managers are responsible for ensuring their team's compliance.
- Staff who fail to follow these policies may face **access suspension or HR review**.
