This document consolidates answers to frequent security questions.

It is intended for ChooseMyCompany clients and partners.
It should not be transfered without the explicit consent of ChooseMyCompany.

Last updated on 29/06/2020

Question ID	Question	Answer	Related documents
	Information security policies		
SEC-DOC-001	ISO/IEC 27001 certification	ChooseMyCompany has an SMSI based on ISO27001/27002. ChooseMyCompany has implemented security measures regarding ISO 27001:2013 requirements (appendix A). We are not aiming for accreditation.	CMC - ISSP -v1.1.docx
	Organization of information security		
SEC-ORG-002	Describe CMC security organization (including responsibilities)	Damien Bénier: CTO, reponsible for Application + Process. Synalabs: responsible for Hosting / Systems. Laurent Labbé: CEO, DPO (CNIL registration: DPO-84637). Celica Thellier: COO	CMC - ISSP -v1.1.docx (chapter 3.2)
SEC-ORG-004	Provide CMC policy regarding the mobile devices	No personal mobile devices can access ChooseMyCompany's infrastructure and systems. In case of access to the professional mailbox on a mobile device, only online solutions can be used. All data and accesses must be deleted on contract's end. Work data (including personal data) can never be stored on a mobile device. Only professional tablets belonging to the company can access the infrastructure and admin interfaces. These devices are registered on the application for 1 year when first activated. They can be deactivated at any time.	
SEC-ORG-005	Indicate how CMC manages the external devices, describe the corresponding policy	No use of external devices (USB keys, external hard drives).	CMC - Charte SSI - vX.X.docx
SEC-ORG-006	Describe how CMC manages major changes in organization and process in terms of security	Due to the size of the company, organizational changes are directly managed by the CEO and the RRH. They ensure roles described in SEC-ORG-002 are attributed	CMC - ISSP -v1.1.docx (chapter 3.2.1 CEO Responsibilities)
	Human resource security		
SEC-HUM-001	Describe how CMC manages secret information (Contract clause, NDA...)	Employees signs a specific clause on data manipulation as part of their work agreement (defining the rules and responsibilities). When CMC uses a service provider, contracts include confidentiality clauses. Partners sign an NDA. In the case of emergency or over-the-counter interventions, an NDA is signed by before the intervention.	CMC - Charte SSI - vX.X.docx
SEC-HUM-002	Describe how CMC manages employees' security awareness and training (particularly regarding security staff, confidential and secret information handling..)	CISO is in charge of planification and managing the awareness & education training session. HR & CISO manage several awareness campaign, on a regular basis. A record of the sessions followed by each employees is maintained.	CMC - Sensibilisation salariés CMC - ISSP -v1.1.docx (chapter 3.2.2 CISO Responsibilities) CMC - ISSP -v1.1.docx (chapter 4.1.HR).
SEC-HUM-003	Indicate how CMC makes sure employees are engaged in a non disclosure agreement to protect confidential or secret information	See SEC-HUM-001 + There exists an ISS charter reminding every user of their respective responsibilities as well as the rules and best practices which need to be applied. This document is signed by all associates, thereby agreeing to the different terms mentioned in the charter. This document is also signed and accepted by all contractors working in ChooseMyCompany's offices.	CMC - ISSP -v1.1.docx (chapter 4.1.HR).

SEC-HUM-004	Provide an overview of CMC on-boarding and off-boarding process (with the agreed delay to disable an account upon contract termination).	Onboarding process : - internal communication - computer configuration and registration - HR onboarding (including ISS charter and NDA signature) - email account creation - ChooseMyCompany account creation - Security training - Interview with the manager of each team - for tech / devs : creation of technical accounts and dev environment Offboarding : - HR offboarding - computer formatting - accounts deactivation (within 3 weeks)	
SEC-HUM-005	Confirm if there is any background verification of employment candidates	The following verifications are performed before hiring and giving access to CMC information systems : - Identification and Verification Checks - Reference - Resume or Curriculum Vitae - Right-to-Work Checks	
SEC-HUM-006	Describe how CMC implements Segregation of Duties and monitor potential conflict of interests	Employees: Work agreement with specific clause Partners: NDA Shareholders: "pacte d'actionnaire"	
SEC-HUM-007	Describe how you define the roles and responsabilities of CMC teams and clients during a project	We defined a RACI (responsible, accountable, consulted, informed) describing the roles of the people involved in a project. This document describes the roles of each CMC teams and the role of the client, for each step of the project (from signature to end of contract).	CMC - Project RACI
	Asset management		
SEC-AST-001	Describe how CMC manages the confidentiality in suppliers' contracts	Supplier contracts include a security provision detailing all confidentiality, availability and integrity obligations as defined in the ISSP's appendix.	
SEC-AST-002	Describe how CMC manages the assets handling client data/information	All assets are listed in an inventory. Each asset is categorized and assigned to an owner.	CMC - Inventaire des actifs
SEC-AST-004	Describe how CMC masters the protection of the information depending on their classification	Rules regulating the use and handling of assets formalized by the classification policy are followed to prevent the disclosure, modification, removal or destruction of all or part of the data, whichever its form and medium may be. Documents are affected to the following classification : - Public: shareable without restriction - Internal: shareable with ChooseMyCompany's associates - Restricted: access restricted to ChooseMyCompany employees working on the subject and clients/partners/contractors on a need-to-know basis - Confidential: cannot be shared outside management without proper clearance.	CMC - SP - Information classification policy -v1.0.docx
SEC-AST-005	Describe how CMC guaranties the destruction of the client information (process, techniques...)	See SEC-CMP-011	Conditions de services.pdf
SEC-AST-006	Describe how CMC manages an end of a contract (process, information destruction techniques...)	Data retention / destruction : SEC-CMP-011 Reversibility : See SEC-CMP-010	Conditions de services.pdf CMC - End of contract
SEC-AST-007	Describe how CMC manages the protection, incident detection for the assets	Server protection : See SEC-OPS-002 Backup : See SEC-OPS-003 and SEC-CRY-003 Logs / traces : See SEC-OPS-004	
SEC-AST-008	Describe how CMC ensures physical destruction of Hard drives	Decommissioned hard drives of production and backup servers are logically destroyed with a software approved by the ANSSI (https://www.ssi.gouv.fr/). After destruction, a signed certificate is emitted to ensure that drives have correctly destroyed with multiple overwritings.	
	Access management		
SEC-ACC-001	Describe how CMC manages access to the platforms from external localization	Access over secured connections only (App access over HTTPS). System level access from Bastion only. Bastion accessible over secured VPN.	CMC - SP - Logical access management policy -v1.1.docx

SEC-ACC-002	Indicate how CMC manages the 'Identity' and provisioning in user access process	Only nominative accounts / use of generic accounts is proscribed. If the conduct of business demands it and if no other solution exists to answer such needs, an exemption request may be sent to the security manager (CISO) for approval. Access controls are periodically reassessed (at least once a year) to ensure their consistency and adequacy with user statuses (position, departures). User accounts related to client organizations (HR accounts, etc.) can be reviewed by the client directly in his backoffice. Accounts can be deleted by written request to the project manager.	CMC - SP - Logical access management policy -v1.1.docx
SEC-ACC-003	Indicate how CMC manages the 'Role' and provisioning in user access process.	The ChooseMyCompany app differentiates several users roles with corresponding access rights. Roles with possible access to the client data : - Super Admin : CMC managers - admin : CMC employees (among with project manager in charge of the client project) - Partner Admin : CMC partner users having access to the surveys of the clients they manage - HR/company : Client HR user accounts - Survey manager : Client sub-account with access to a specific survey or a subpart of a survey Resources access rights management is based on the principle of least privilege. Users are given the smallest number of privileges required for the accomplishment of their missions.	CMC - SP - Logical access management policy -v1.1.docx CMC - User accounts management
SEC-ACC-004	Indicate how you manage the 'Authentication' in your user access process.	In accordance with ChooseMyCompany's ISSP, all account are nominative (no generic accounts). Authentication on the application is done over HTTPS with email and password. ChooseMyCompany also supports SSO authentication, via the SAML2 protocol. Passwords are defined by the users and must follow the following policy : - all accounts (default) : 8 chars, 3 different charsets - admin accounts: 12 chars, 3 different charsets, expires after 6 months - client accounts: follow default policy, but can be reinforced according to client policy/needs Password are never stored in clear. They are hashed with a random individual salt before they are stored in database. On account creation, the user receives an email with a temporary activation link. This link redirects the user on a page where he/she must define his/her password (in accordance with its account type policy) before he/she can log in. In case of forgotten password, a temporary link can be sent to the account email address, in order to let the user define a new password (always according to its account policy). Complementary protection systems : - Anti-brute force filter Connections - failed connections recording. In the event of an application audit, temporary accounts, consistent with the type of conducted audit (but never an administrator account) can be attributed for the auditors. At system level, only SSH access from defined bastions is possible. SSH authentication is done via individual SSH RSA keys.	CMC - SP - Logical access management policy -v1.1.docx CMC - Authentication
SEC-ACC-005	Describe how a client/partner can reinforce the password policy for its users	Each client / partner can decide to reinforce the password policy for its users. The password policy can define the following parameters : - "minLength": minimum password length - "historySize": number of previous passwords that cannot be reused - "expiration": period on password validity (after which it must be renewed) - "passwordTokenValidity": duration of the token in password renewal email messages - "characterSets": expected character sets contained in the password ('figure', 'lower', 'upper', 'special')	CMC - Authentication
SEC-ACC-006	Describe how CMC masters the access to sensitive platforms or information	Few people can access such information ("Need to know" principle according to the policy). - Personal (non generic) accounts only. - Several roles : See SEC-ACC-003. - Documents classification : See SEC-AST-004 - Server access protection : See SEC-OPS-002	

SEC-ACC-007	Describe CMC password policy	Application : See SEC-ACC-004 Passwords must never appear in clear text anywhere (programs, files, scripts, traces or logs) . Users are made aware of all password rules.	CMC - SP - Logical access management policy -v1.1.docx CMC - Authenitification
SEC-ACC-010	Describe how CMC manages the access to data received from a transfer	Datasets containing personal data can only be transfered (and stored) via secured application where an expiration/deletion date can be defined. When needed, other transfered data can be stored localy on user encrypted/protected machines for the duration of the corresponding work only. + SEC-COM-004	
SEC-ACC-011	What is implemented to prevent data leaks ?	All account are nominative and access to customer survey data on the plateform is logged. Employees sign an IT security charter. Employees and subcontractors sign an NDA when affected on projects. No external storage is allowed. (See SEC-ORG-005)	CMC - Charte SSI - vX.X.docx
SEC-ACC-012	Describe how CMC manages Shared Ids (e.g. root, Sys, System, etc.), Group IDs (generic accounts used by several individual belonging to a same team for example).	Nominative accounts are always used when possible (See SEC-ACC-004). When not possible, generic accounts can be used within an ssh session opened with a nominative certificate. The ChooseMyCompany tech/dev team can only access application level of the servers. System / Network equipments can only be accessed by system administrators. When a person quits the team, all accesses are deleted as described in our Offboarding procedure.	
	Cryptography		
SEC-CRY-002	Precise how CMC manages the encryption	Data / documents must be encrypted according to their classification (See SEC-AST-004). All transfers are secured by protocol (HTTPS, SSH, etc.). SSL : https://www.ssllabs.com/ssltest/analyze.html?d=choosemycompany.com&hideResults=on (end of support for TLS 1.0 and TLS 1.1 on 31/08/2020) Work station hard drives are encrypted by OS (XTS AES 128 bits). Personnal data on production servers are encrypted in Databases (AES-256-CBC). Sensitive data must be encrypted before it is transfered (especially health and private information). Data can be encrypted via the following tools: PGP, S/MIME, Archives Zip, etc.	CMC - SP - Encryption policy -v1.0.docx
SEC-CRY-003	Describe CMC backup policy	Backup images are created 24 times a day, encrypted with AES 256, and stored on separate datacenter. Backup images integrity is checked every week. Backup images are kept for 3 months.	CMC - Backup policy
	Physical and environmental security		
SEC-PHY-001	Indicate CMC's level of hosting physical security (Datacenter certification)	DC3 (prod A), DC5-A (prod B) and DC2 (backup) Data centers (online SAS, Groupe Illiad). Certifications : ISO 27001, 50001, HDS	https://www.scaleway.com/datacenter/
SEC-PHY-002	Describe where CMC's data is hosted (where are Datacenters located)	PROD Site A: Datacenter : Iliad Entreprise DC5-A, Infrastructure Online.net, Nanterre, Salle : 120 120, Baie : B11, PROD Site B: Datacenter : Iliad Entreprise DC3, Infrastructure Online.net, Vitry-sur-Seine, Salle : 4 4-6, Baie : A14 Stockage des sauvegardes: Iliad Entreprise DC2, Infrastructure Synalabs, Vitry-sur-Seine, Salle 204-B, Baie: C1	
SEC-PHY-003	Describe how CMC manages the different physical zones according to their level of criticity	Each office is divided into physical security areas. Three types of physical security areas are identified: - Public lobby - Internal areas - access limited to employees, collaborators and accompanied visitors (ex: offices, meeting rooms, training rooms, etc). - Access-restricted areas - limited to individuals with proper authorization (ex: HR documents storage) Confidential documents stored in a physical safe. ChooseMyCompany's offices located at 56 rue des Batignolles, Paris, France. Access is restricted by auto closing door, unlocked by nominative badge Visitor acceses logged with name and date / time.	CMC - SP - Physical access management policy -v1.1.docx CMC - Plan Locaux rue des Batignolles.png

SEC-PHY-004	Describe how physical access to CMC servers is managed	Production datacenters (DC3 (prod A), DC5-A (prod B) and DC2 (backup) Data centers, online SAS, Groupe Illiad) follow best security practices : - Secured loading docks - 24x7 on-site security guard - Internal and External CCTV with complete site coverage - Biometric scan & RFID badges - Water mist system - VESDA smoke detectors	CMC - SP - Physical access management policy -v1.1.docx
SEC-PHY-005	Indicate how CMC is protected against natural threats	Physical security measures against fire, flooding, earthquakes, explosions, civil unrest and other catastrophes (natural or man-made) have been identified and are applied. (ex: fire extinguishers) Data centers operatesspecific physical security measures and comply with ChooseMyCompany requirements.	CMC - Management of environmental risks
	Operations security		
SEC-OPS-001	Indicate how the different environments (Development, testing, production) are organized	- Development environment runs in Docker containers on local machines. It uses fixtures data. - Testing / Continuous integration runs on specific servers. It uses fixtures data. - Pre-production servers runs in VMs in a private cloud. - Production servers runs in VMs in a private cloud. - Failover productions servers uses in a separate data center. Data: See SEC-ACQ-001	CMC - Development workflow
SEC-OPS-002	Describe how CMC manages endpoint protection	Employees machines hard-drives are encrypted and have an Antivirus solution installed. Production servers are secured with: Firewall : - blocks all traffic except HTTP (and SSH from bastion) - blocks IP options, SMURF, Ping of Death, large packet attacks Reverse Proxy (HA Proxy) : - lets only valid HTTP requests pass - blocks TCP SYN Flood, DDOS Gigabit connection: - Over provisioning / prevents traffic flooding attacks…	CMC - Charte SSI - vX.X.docx
SEC-OPS-003	Describe how CMC manages backups	See SEC-CRY-003	
SEC-OPS-004	Describe how CMC manages event logs	ChooseMyCompany records logs log at different levels : - SSH auth logs - web access logs - system logs (syslog) - application authentication logs - application operation logs Logs are only accessible by users with administration privileges. A back-up of the logs is systematic, during the global back-up process. Logs are centralized in a log management system. In case of incident, logs are analyzed in order to trace the events leading to the problematic situation. When needed, relevant logs can be provided to the client.	
SEC-OPS-005	Indicate how CMC monitors non-authorized administration activities	People are assigned privileges according to their roles (at application level and at system level). Administration activities are limited to specific people with respect to the least privilege principle. Administration activities are traced in logs and are reviewed on suspicion: see SEC-OPS-004.	
SEC-OPS-006	Describe CMC's vulnerability management process	ChooseMyCompany manages its vulnerabilities through: - Continuous patch management : see SEC-OPS-008. - Periodic logs review : see SEC-OPS-004 - External penTests : see SEC-OPS-010	
SEC-OPS-007	Describe CMC's timeline to fix identified vulnerabilities	Each potential identified vulnerability will be qualified as minor, major and critical. - Critical vulnerabilities will be treated with high priority (within 2 weeks) - Major vulnerabilities will be treated within 2 months - Minor vulnerabilities will be treated within 6 months	
SEC-OPS-008	Describe CMC's patch management process	Third party softwares / libraries used in the system are checked against vulnerability databases. In case of security failure, released patches will be applied: - System : Critical patches are applied within 48h after release. - External application libraries : Critical patches are applied within 2 weeks after release.	

SEC-OPS-009	Describe the change management in place and how changes performed are monitored and logged	All modifications/updates to the config are versioned in a GIT repository. New versions are automatically provisioned. - System : Machines are provisioned via Puppet. - Application : Code is deployed via deployment scripts Specific checks before and after changes ensure the change is performing as expected. Continuous monitoring ensures that no regression is induced by changes. Developement lifecycle: See SEC-ACQ-002	
SEC-OPS-010	Is CMC system's security checked by external companies?	External Pentests carried out by ANSSI recommended companies to audit the application security. Clients can also also carry out their own Pentests (at their own expenses, while respecting the notice period). After each test, correction of possible discovered vulnerabilities is planned : See SEC-OPS-007 + SEC-OPS-008	
SEC-OPS-011	How does CMC ensures all systems have a common time reference?	Synchronisation via NTP	
SEC-OPS-012	Describe how firewalling and vulnerability assessments accommodating the virtualization technologies is performed (e.g. virtualization aware)	Firewalling is not part of the virtualization infrastructure. Filtering of incoming streams is performed by an appliance firewall (pfSense FreeBSD) dedicated to this usage.	
SEC-OPS-013	What type/model of Firewall are implemented to segregate security zones internally and to protect the infrastructure from external attacks	pfSense FreeBSD	
SEC-OPS-014	Describe what is in place to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.) and the technical controls in place to prevent them.	Hypervisor BIOS (Dell servers) and kernels are up to date. (in particular to workaround Intel processor flaws)	
SEC-OPS-015	Provide the detailed Technical Architecture description of all the components of the proposed solution including monitoring solutions used by the provider	The CMC application runs on a Private cloud. Virtualization: Proxmox / Linux KVM hypervisor OS: Debian HTTP layer: HAProxy / Varnish / Apache Application: PHP / NodeJS / Python (+ VueJS on the front part) Storage: MySQL / ElasticSearch Async Queuing: RabbitMQ Backup: R1Soft Monitoring: Sentry / AppBeat / DataDog	
SEC-OPS-016	Provide an overview of the various standards, methodologies, tools, policies and processes in place to support service operations	CMC implements an SMSI based on ISO 27001/2. Operation support can be split into 3 levels : - project management : functional support - developement : technical application support - hosting : system / infrastructure support	
SEC-OPS-017	All workstation are protected with an anti-virus solution. The solution's virus database must have automatic update activated (minimal frequency: daily). The user must in no occasion deactivate the solution. Servers system do not use anti-virus solutions. These are unix systems that benefit from the security intrinsic to these systems (users separation, execution rights, etc.).	All workstation are protected with an anti-virus solution. The solution's virus database must have automatic update activated (minimal frequency: daily). The user must in no occasion deactivate the solution.	CMC - Charte SSI - vX.X.docx
	Communications security		
SEC-COM-001	Describe how CMC manages access to client's data (including from external localization)	Data is accessed over secured connection (HTTPS for the application). Client data is only accessible by authorized CMC employees. No work data can be stored on any personal device: see SEC-ORG-004 + SEC-ORG-005 Local data storage: See SEC-ACC-010	
SEC-COM-002	Describe how CMC manages its network protection	See SEC-OPS-002	
SEC-COM-003	Describe CMC network segregation strategy	- Production and pre-production environments are isolated and independent from other networks (firewall enabling only HTTP/S access) - System level access to production / pre-production machines is done from bastion (accessed via secured VPN) - Backup machines are isolated and independent from other networks - Development environment is local with no public access (dev env only uses fixture data)	

SEC-COM-004	Describe how CMC protects the data during a transfer (internal or external).	All data are transferred over secured channels : - HTTPS for web transfers - SMTPS for email transfers (PGP or S/MIME if available on client side) - SFTP for direct file transfers - SSH for system administration In case of technical impossibility to use a secured channel, the information itself must be encrypted. Here are the main data transfers of the application and the corresponding securisation / encryption : - Between prod master and prod slave : DRBD over TCP on a private network / VLAN - Between prod and backup : RSA and AES encyption (R1soft solution) - Between prod and preprod environments : scp - Between prod and customer's system : to be defined if necessary. - Between prod and users (customer users in particular) : HTTPS. - Between prod and technical admin users : SSH (from bastion)	
	Systems acquisition, development and maintenance		
SEC-ACQ-001	Indicate how CMC handles the different data needed in the different environments (Development, testing, production)	Development environments use only fixtures Data. Automated test environments use only fixtures Data. Pre-production environment has the same level of security as production and uses the same data (replicated nightly).	
SEC-ACQ-002	Describe how CMC manages security during the development lifecycle	Specifications : - Functional specifications defined by the Product Owner - Technical specifications defined by a senior developer / architect - If personal data at stake, PIA and update of the GDPR “register of processing operations” (Registre des traitements) Development : - Development on local environment using only fixture data - Submission of Code changes in a Pull Request - Review and validation of the Pull Request by a second Developer - Automatic start of Continuous Integration to run Unit and functional tests + static code analysis. Validation : - Deployment of the feature on the preproduction environment - Human validation of the features (by the Product Owner) on a preproduction environment - Deployment in production	CMC - Development Workflow
SEC-ACQ-003	What automatic verifications are performed on CMC application code	- automated unit and functional tests - static code analysis of all server side code with PHP Stan - dependencies vulnerability verification with Github "Security vulnerabilities reports"	https://help.github.com/en/github/managing-security-vulnerabilities/about-security-alerts-for-vulnerable-dependencies
SEC-ACQ-004	Confirm that no client operational data is used for testing	Confirmed. See SEC-ACQ-001	
SEC-ACQ-005	Describe how CMC tenants can report Bugs and security vulnerabilities and the process in place to remedy reported defects.	Bugs and security vulnerabilities are reported to the project manager. The project manager priorize the need with the team lead. The prioritized needs are planned with the tech team. The tech teams develops and releases the feature (with validation of the project manager). The project manager notifies the client. Security fixes: See SEC-OPS-007 Security patches: See SEC-OPS-008	
	Third party relationship		
SEC-SUP-010	Give the list of CMC sub-contractors	Infogérance : - Synalabs : France, SIRET 50217842900036, 103 Rue Réaumur, 75002 Paris Hebergement : - Synalabs, sur des serveurs Online SAS (See SEC-PHY-002) Envoi d'emails : - Mailjet : France, SIRET 52453699200059, 13-13 bis, rue de l’Aubrac – 75012 Paris. Serveurs localisés à Francfort en Allemagne et St. Ghislain en Belgique	
SEC-SUP-001	Indicate how CMC masters the information and access segregation of your different customers (Data Isolation / Data segregation)	All accounts are nominative and assigned minimum privileges to conduct its duty. Data segregation is applicative: - 2 levels of security checks implemented in the application : high level check of the user rights on the request + low-level lock of user rights on the accessed data - PenTest conducted by ANSSI recommended companies, including specific focus on data segregation.	
SEC-SUP-002	Indicate how CMC can provide capability to dedicate environment to the client and limits (if any)	The client has access to dedicated backoffices to manage its data. Logical separation.	

SEC-SUP-003	Indicate how CMC can manage applications in the client environnement	ChooseMyCompany provides a web SaaS solution. Only a standard browser is needed.	
SEC-SUP-004	Describe how CMC manages the changes linked to security (communication to users, renewal of certifications...)	Project manager are informed of important security updates and will communicate it to their clients. Continuous/incremental security improvements are not subject to specific communication. In case of specific processes needed by the client, such information must be written on the linked contract. Change management: See SEC-OPS-009	
SEC-SUP-005	Indicate how CMC chooses its third parties and make sure they are compliant with customers' security rules.	CMC chooses expert third parties that can satisfy and engage their compliance with CMC requirement, in particular concerning security aspects. The contractors are benchmark and selected on these criterias. Contract clause: See SEC-SUP-006	
SEC-SUP-006	Indicate how CMC makes sure your subcontractors are engaged in a non disclosure agreement to be compliant with its customers' security requirements	Subcontractors contract include an NDA clause.	CMC - Subcontractors contractual clause
	Information security incident management		
SEC-INC-001	Does CMC have a security incident management process ?	We have a security incident management process detailing: - The different roles and responsibilities involved in security incident management - The principles of security incident classification (typology and levels of significance) - The various stages of security incident management (explaining which tools to use and which actions to take) Security incidents are reported to, as well as registered and archived by the CISO.	CMC - SP - Security incident management policy -v1.1.docx
SEC-INC-002	Describe CMC's security incident management process.	1) incident detection (gather basic information. If personal Data impacted, specific GDPR process) 2) Incident classification (Critical / High / Medium / Low) 3) Incident analysis (logs analysis, etc.) 4) Action decision : Containment / Recovery 5) Communication if external parties are concerned (clients, partners) 6) Improvement measures / correction planification	CMC - SP - Security incident management policy -v1.1.docx
SEC-INC-003	Describe how users (employees, contractors, clients) can report security weaknesses in system or services.	See SEC-ACQ-005	
SEC-INC-004	Describe how clients can report issues.	A project manager is assigned to each client project To report an issue: - the client can contact the project manager (by phone or email) - the survey manager will reply to the client (SLA 24h) - in case of complex request, it will be escalated to the "head of production" - if the "head of production" identifies a technical problem, the query is transfered to the technical team. After analysis, if the request is identified as critical, it ill be processed in priority. Otherwise it will be planned and an estimate fix date is communicated to the client : See SEC-OPS-007 + SEC-OPS-008	
	Business continuity management		
SEC-BCP-001	Describe CMC's Disaster Recovery Plan and Business Continuity Plan process	All elements required for recovery to occur in compliance with business needs and contractual business continuity obligations (time, data loss) are implemented and carried out by either ChooseMyCompany or its providers. ChooseMyCompany's reliable architecture is based on full redundancy of our Production servers in separate datacenters (active / passive with realtime replication). SLA : 99% RTO : 5h RPO : 3h In the event of an incident impacting the availability of resources, the CTO and COO keep affected clients updated on the impacts and their possible evolution.	CMC - Business Continuity - Disaster Recovery.docx CMC - Backup Policy
SEC-BCP-002	Provide an overview of how capacity planning is managed to limit the risk of system overload and what are the allowances/restriction of use of oversubscription capabilities present in the Hypervisor for customers. Also indicate how capacity planning and usage information is communicated to the customer.	Systems usage (memory, CPU, etc.) are monitored and trigger an alert in case of threshold reached. System administrators will then take the appropriate action to provision the new machines.	
SEC-BCP-003	What is CMC's process to monitor that system performance continuously meets all requirements (contractual, business, regulatory) to provide proper service to your customers. Can the customer run his own performance measurement?	We use external tools to monitor application uptime (Datadog, Appbeat, Graylog). The customer can run his own performance measurement.	
	Compliance		

SEC-CMP-002	Describe how CMC manages personal data and compliancy with privacy related laws or regulation (Europe)	GDPR Compliant. Worked on conformity in 2018 with an external consulting company. Designation of a DPO. All Data are stored in France. Personal data (like email addressess) are encrypted in Database.	
SEC-CMP-003	Describe how CMC manages the compliance with the laws of the different involved countries	CMC relies on an external legal experts. Application and processes can be adapted for specific local laws.	
SEC-CMP-005	Describe CMC's ISMS review and audit process	CMC does not target formal ISO27001 certification. Regular reviews, following internal or external (client / partner) feedbacks imply continuous improvement of the security tools, rules and processes.	
SEC-CMP-006	Describe CMC's internal audit organization with a focus on the ISSP check	Due to its size, CMC does not have an internal audit organization. If needed, CMC reserves the right to rely on subcontractors for audits.	
SEC-CMP-007	GDPR Compliance / Application of rights	All personal data treatments are recorded in the register of processing operations ("Registre des traitement"). Application of "Security by default" and "Privacy by design" principles. Recording of user right application requests. Process defined to handle user requests / application of rights. Designation of a DPO.	CMC_RegistreDesTraitements_V1.0.xlsx CMC - Procédure d'application des droits-v1.0.docs CMC - GDPR Compliance Statement-V1.2.docx
SEC-CMP-008	Describe the process in place for the customers to gain access to their personal data as required by the EU regulations (GPDR)	A contact form with a specific GDPR request possibility is available to all visitors / users. The request can also be sent directly to dpo@choosemycompany.com. The process is the following : - request received by the DPO - DPO validates request - DPO informs requester that request is being processed - Project Manager and/or CTO process the request / required actions - Project Manager and/or CTO notifies DPO	CMC - Procédure d'application des droits-v1.0.docs
SEC-CMP-012	Describe the cookies policy of CMC	Visitor's consent is required before setting a cookie. Given consents can be edited at any time from the user profile (or the website footer). ChooseMyCompany uses cookies for : - technical navigation (storage of current langage, sessionId) - visitor participation (ask visitor to take part in a spontaneous survey and mark his/her participation) - "Remember Me" (storage of th last used account to ease the log in process) - Traffic Analysis (we rely on the Google Analytics solution)	https://choosemycompany.com/fr/cookies-policy
SEC-CMP-009	Describe CMC measures to protect surveyed users anonymity (anonymization principles).	- Unless specific contractual clause, data collected by CMC belongs to CMC. They are stored for 5 years as is and then all ids relating to the client are destructed. - Email addresses (personal data) of participants are destroyed after 12 months by default (configurable). - User accounts are reviewable by the client and can be deactivated or destructed on demand. - User accounts with no activity during 1 year are automaticaly deactivated. - User accounts deactivated for 1 year are automaticaly anonymized (deletion of all personal data). These operation automatically performed on the productions databases on a daily basis. Les logs sont stockés sur les machines qui les génèrent pendant les durées suivantes : - logs applicatifs sont conservés 11 semaines - logs d'accès web sont conservés pendant 14 jours - logs d'authentification SSH sont stockés pendant 4 semaines - logs systèmes courants (syslog) pendant 7 jours Ces logs sont également centralisés dans un SIEM où ils sont conservés pendant 1 an Encrypted backup images are store for 3 months	
SEC-CMP-090	Describe in more details the mechanism used to prevent sending useless reminder emails while preserving respondents anonymity	Each email sent to an invitee contains a link to participate to the survey. This link contains a unique identifier (different for each invitee). When clicking it, the identifier is added to the questionnaire. When submitting the questionnaire: - the identifier is used to recognize the invitee and increment its submissions count (and hence, not send him/her additional reminder emails). - the participant answers are stored in a separate database with no link to the invitee unique identifier. Hence, there is no way to relate the participant answers to the invitee (the email adress of the surveyed participant).	

SEC-CMP-010	Describe how reversibility is addressed (end of contract).	ChooseMyCompany, as part of its service, protects the anonymity of the survey participants and hence can not provide all the collected data to the client. Available Data : - Collected data (answers) after aggregation and anonymization - Classification datas (qualitative analysis) - Information about invited participants (before they are destroyed) - Information on project management Format : JSON / CSV Delay : in the 3 months following the end of the contract.	CMC - End of contract
SEC-CMP-011	Describe CMC Data retention policy.	- Unless specific contractual clause, data collected by CMC belongs to CMC. They are stored for 5 years as is and then all ids relating to the client are destructed. - Email addresses (personal data) of participants are destroyed after 12 months by default (configurable). - User accounts are reviewable by the client and can be deactivated or destructed on demand. - User accounts with no activity during 1 year are automaticaly deactivated. - User accounts deactivated for 1 year are automaticaly anonymized (deletion of all personal data). These operation automatically performed on the productions databases on a daily basis. Les logs sont stockés sur les machines qui les génèrent pendant les durées suivantes : - logs applicatifs sont conservés 11 semaines - logs d'accès web sont conservés pendant 14 jours - logs d'authentification SSH sont stockés pendant 4 semaines - logs systèmes courants (syslog) pendant 7 jours Ces logs sont également centralisés dans un SIEM où ils sont conservés pendant 1 an Encrypted backup images are store for 3 months	CMC - Stockage des données / Data retention