No.	Control Name	Low-Impact	Moderate-Impact	High-Impact	Action taken / Notes
AC-1	POLICY AND PROCEDURES	AC-1	AC-1	AC-1	Creation of a document in points with the high-level policies concerning the CA, with functions allowed to the single roles, scopes and resources
AC-2	ACCOUNT MANAGEMENT	AC-2	AC-2 (1) (2) (3) (4) (5) (13)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)	Role identification. Security admin account management policy. There are no groups, the role is defined on the basis of the transactions that it performs. The admin is the only one who can add chat rooms or delete them. Access to the system is governed by username and password to all users. There are no group accounts, they are personal
AC-3	ACCESS ENFORCEMENT	AC-3	AC-3	AC-3	Users have to sign up by passing their username, password and repeat password. After filling in this information, the data is saved in sqlite databse. Password are encrypted thanks to Django encryption methods. The next step is Log in to access the website. Users have 2 choices: 1) Log in using their credentials or 2) Log in using Google authentication.
AC-4	INFORMATION FLOW ENFORCEMENT		AC-4	AC-4 (4)	The information contained in the database and the tokens travel only on https encrypted channels. Critical information such as passwords etc. are encrypted by Django password encryption, to avoid SQL injection attacks and the like.
AC-5	SEPARATION OF DUTIES		AC-5	AC-5	User of the chat can only enter available chat rooms and write messages. Admin of the page can add and remove rooms and has all functionality that a user has.
AC-6	LEAST PRIVILEGE		AC-6 (1) (2) (5) (7) (9) (10)	AC-6 (1) (2) (3) (5) (7) (9) (10)	The roles have been structured in such a way that only the users of interest have access to the resources and furthermore each role has been given only the strictly necessary permissions. Unprivileged (unauthenticated) users have no visibility into security features.
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	AC-7	AC-7	AC-7	If there is an unsuccessful logon attempt, user has another attempts to try to log in. User has 5 attempts in total. It is implemented in order to prevent application brute force attacks. It uses django-axes and blocks application. Also there is "cool-off period" this dictates how long you will have to wait before you can try logging into website again. Value that is set is 1 hour
AC-8	SYSTEM USE NOTIFICATION	AC-8	AC-8	AC-8	-
AC-10	CONCURRENT SESSION CONTROL			AC-10	-

AC-11	DEVICE LOCK		AC-11 (1)	AC-11 (1)	The OS must foresee that, after a certain period of time, access to the machine is blocked and information inaccessible
AC-12	SESSION TERMINATION		AC-12	AC-12	Access tokens have a limited duration, and furthermore, regardless of the duration of the token, the session has a limited duration, and has different times for an idle and an active session. Configuartion of access token duration can be configured in Django
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14	AC-14	AC-14	There isn't any action or URL that is accessible without identification or authentication. In order to gain access to the website, user has to sign up and then log in or authenticate itself using Google authentication
AC-17	REMOTE ACCESS	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)	The system consists of a web server and of sqlite database that is located on the same subnet as the backend with which it must communicate
AC-18	WIRELESS ACCESS	AC-18	AC-18 (1) (3)	AC-18 (1) (3) (4) (5)	Wireless access has not been checked
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	AC-19	AC-19 (5)	AC-19 (5)	This is a website, so there is no need in additional access control for mobile devices. They are treated in the same way as a casual PC user
AC-20	USE OF EXTERNAL SYSTEMS	AC-20	AC-20 (1) (2)	AC-20 (1) (2)	Data cannot be moved to external information systems. The only information shared with an external service could be domain name, username, chat rooms and their content
AC-21	INFORMATION SHARING		AC-21	AC-21	-
AC-22	PUBLICLY ACCESSIBLE CONTENT	AC-22	AC-22	AC-22	All the content that is in each room is publicly available. The information contained on the front page, rooms and in each room is public. Creating new room, deleting existing room and kicking out the user is accessible only by the admin
AT-1	POLICY AND PROCEDURES	AT-1	AT-1	AT-1	-
AT-2	LITERACY TRAINING AND AWARENESS	AT-2 (2)	AT-2 (2) (3)	AT-2 (2) (3)	-
AT-3	ROLE-BASED TRAINING	AT-3	AT-3	AT-3	-
AT-4	TRAINING RECORDS	AT-4	AT-4	AT-4	-
AU-1	POLICY AND PROCEDURES	AU-1	AU-1	AU-1	-
AU-2	EVENT LOGGING	AU-2	AU-2	AU-2	-
AU-3	CONTENT OF AUDIT RECORDS	AU-3	AU-3 (1)	AU-3 (1)	-
AU-4	AUDIT LOG STORAGE CAPACITY	AU-4	AU-4	AU-4	-
AU-5	RESPONSE TO AUDIT LOGGING PROCESS FAILURES	AU-5	AU-5	AU-5 (1) (2)	-
AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)	-
AU-7	AUDIT RECORD REDUCTION AND REPORT GENERATION		AU-7 (1)	AU-7 (1)	-
AU-8	TIME STAMPS	AU-8	AU-8	AU-8	-
AU-9	PROTECTION OF AUDIT INFORMATION	AU-9	AU-9 (4)	AU-9 (2) (3) (4)	-

AU-10	NON-REPUDIATION			AU-10	-
AU-11	AUDIT RECORD RETENTION	AU-11	AU-11	AU-11	-
AU-12	AUDIT RECORD GENERATION	AU-12	AU-12	AU-12 (1) (3)	-
CA-1	POLICY AND PROCEDURES	CA-1	CA-1	CA-1	-
CA-2	CONTROL ASSESSMENTS	CA-2	CA-2 (1)	CA-2 (1) (2)	-
CA-3	INFORMATION EXCHANGE	CA-3	CA-3	CA-3 (6)	-
CA-5	PLAN OF ACTION AND MILESTONES	CA-5	CA-5	CA-5	-
CA-6	AUTHORIZATION	CA-6	CA-6	CA-6	-
CA-7	CONTINUOUS MONITORING	CA-7 (4)	CA-7 (1) (4)	CA-7 (1) (4)	-
CA-8	PENETRATION TESTING			CA-8 (1)	-
CA-9	INTERNAL SYSTEM CONNECTIONS	CA-9	CA-9	CA-9	-
CM-1	POLICY AND PROCEDURES	CM-1	CM-1	CM-1	-
CM-2	BASELINE CONFIGURATION	CM-2	CM-2 (2) (3) (7)	CM-2 (2) (3) (7)	-
CM-3	CONFIGURATION CHANGE CONTROL		CM-3 (2) (4)	CM-3 (1) (2) (4) (6)	-
CM-4	IMPACT ANALYSES	CM-4	CM-4 (2)	CM-4 (1) (2)	-
CM-5	ACCESS RESTRICTIONS FOR CHANGE	CM-5	CM-5	CM-5 (1)	-
CM-6	CONFIGURATION SETTINGS	CM-6	CM-6	CM-6 (1) (2)	-
CM-7	LEAST FUNCTIONALITY	CM-7	CM-7 (1) (2) (5)	CM-7 (1) (2) (5)	-
CM-8	SYSTEM COMPONENT INVENTORY	CM-8	CM-8 (1) (3)	CM-8 (1) (2) (3) (4)	-
CM-9	CONFIGURATION MANAGEMENT PLAN		CM-9	CM-9	-
CM-10	SOFTWARE USAGE RESTRICTIONS	CM-10	CM-10	CM-10	-
CM-11	USER-INSTALLED SOFTWARE	CM-11	CM-11	CM-11	-
CM-12	INFORMATION LOCATION		CM-12 (1)	CM-12 (1)	-
CP-1	POLICY AND PROCEDURES	CP-1	CP-1	CP-1	-
CP-2	CONTINGENCY PLAN	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (5) (8)	-
CP-3	CONTINGENCY TRAINING	CP-3	CP-3	CP-3 (1)	-
CP-4	CONTINGENCY PLAN TESTING	CP-4	CP-4 (1)	CP-4 (1) (2)	-
CP-6	ALTERNATE STORAGE SITE		CP-6 (1) (3)	CP-6 (1) (2) (3)	-
CP-7	ALTERNATE PROCESSING SITE		CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)	-
CP-8	TELECOMMUNICATIONS SERVICES		CP-8 (1) (2)	CP-8 (1) (2) (3) (4)	-
CP-9	SYSTEM BACKUP	CP-9	CP-9 (1) (8)	CP-9 (1) (2) (3) (5) (8)	-
CP-10	SYSTEM RECOVERY AND RECONSTITUTION	CP-10	CP-10 (2)	CP-10 (2) (4)	-
IA-1	POLICY AND PROCEDURES	IA-1	IA-1	IA-1	The document contains the identification and authentication policies for the various roles. (login and password and Google Authentication). Identification and authentication are both implemented Django default Login Views. Authentication for launching the software is via password
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	A-2 (1) (2) (8) (12	IA-2 (1) (2) (8) (12)	IA-2 (1) (2) (5) (8) (12)	Authentication takes place by logging into the website by passing username and password. The web server uses the temporary access token for client identification for policy enforcement
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION		IA-3	IA-3	-
IA-4	IDENTIFIER MANAGEMENT	IA-4	IA-4 (4)	IA-4 (4)	-

IA-5	AUTHENTICATOR MANAGEMENT	IA-5 (1)	IA-5 (1) (2) (6)	IA-5 (1) (2) (6)	At the time of registration all the standards regarding the use of passwords are imposed, in particular regarding the minimum length 8, that the last 3 passwords cannot be used, and that at least one upper case character and one special character must be entered. Also Django checks for common passwords if such one occurs then website will promt user to enter it once again. Also password is validated in order to prevent password and username similarities
IA-6	AUTHENTICATION FEEDBACK	IA-6	IA-6	IA-6	Password fields show stars and don't show plaintext fields. If I don't have an authorization, the web server replies 403 or 401 without specifying the cause. Django shows the user warning if the password is to easy while creating it. When a database does not authenticate a user it does not specify why but only answers access denied
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-7	IA-7	IA-7	-
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	IA-8 (1) (2) (4)	IA-8 (1) (2) (4)	IA-8 (1) (2) (4)	Not necessary, users outside organization have access to the public page only and web chat rooms
IA-11	RE-AUTHENTICATION	IA-11	IA-11	IA-11	-
IA-12	IDENTITY PROOFING		IA-12 (2) (3) (5)	IA-12 (2) (3) (4) (5)	-
IR-1	POLICY AND PROCEDURES	IR-1	IR-1	IR-1	-
IR-2	INCIDENT RESPONSE TRAINING	IR-2	IR-2	IR-2 (1) (2)	-
IR-3	INCIDENT RESPONSE TESTING		IR-3 (2)	IR-3 (2)	-
IR-4	INCIDENT HANDLING	IR-4	IR-4 (1)	IR-4 (1) (4) (11)	-
IR-5	INCIDENT MONITORING	IR-5	IR-5	IR-5 (1)	-
IR-6	INCIDENT REPORTING	IR-6	IR-6 (1) (3)	IR-6 (1) (3)	-
IR-7	INCIDENT RESPONSE ASSISTANCE	IR-7	IR-7 (1)	IR-7 (1)	-
IR-8	INCIDENT RESPONSE PLAN	IR-8	IR-8	IR-8	-
MA-1	POLICY AND PROCEDURES	MA-1	MA-1	MA-1	-
MA-2	CONTROLLED MAINTENANCE	MA-2	MA-2	MA-2 (2)	-
MA-3	MAINTENANCE TOOLS		MA-3 (1) (2) (3)	MA-3 (1) (2) (3)	-
MA-4	NONLOCAL MAINTENANCE	MA-4	MA-4	MA-4 (3)	-
MA-5	MAINTENANCE PERSONNEL	MA-5	MA-5	MA-5 (1)	-
MA-6	TIMELY MAINTENANCE		MA-6	MA-6	-
MP-1	POLICY AND PROCEDURES	MP-1	MP-1	MP-1	-
MP-2	MEDIA ACCESS	MP-2	MP-2	MP-2	-
MP-3	MEDIA MARKING		MP-3	MP-3	-
MP-4	MEDIA STORAGE		MP-4	MP-4	-
MP-5	MEDIA TRANSPORT		MP-5	MP-5	-
MP-6	MEDIA SANITIZATION	MP-6	MP-6	MP-6 (1) (2) (3)	-
MP-7	MEDIA USE	MP-7	MP-7	MP-7	-

PE-1	POLICY AND PROCEDURES	PE-1	PE-1	PE-1	-
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	PE-2	PE-2	PE-2	-
PE-3	PHYSICAL ACCESS CONTROL	PE-3	PE-3	PE-3 (1)	-
PE-4	ACCESS CONTROL FOR TRANSMISSION		PE-4	PE-4	-
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES		PE-5	PE-5	-
PE-6	MONITORING PHYSICAL ACCESS	PE-6	PE-6 (1)	PE-6 (1) (4)	-
PE-8	VISITOR ACCESS RECORDS	PE-8	PE-8	PE-8 (1)	-
PE-9	POWER EQUIPMENT AND CABLING		PE-9	PE-9	-
PE-10	EMERGENCY SHUTOFF		PE-10	PE-10	-
PE-11	EMERGENCY POWER		PE-11	PE-11 (1)	-
PE-12	EMERGENCY LIGHTING	PE-12	PE-12	PE-12	-
PE-13	FIRE PROTECTION	PE-13	PE-13 (1)	PE-13 (1) (2)	-
PE-14	ENVIRONMENTAL CONTROLS	PE-14	PE-14	PE-14	-
PE-15	WATER DAMAGE PROTECTION	PE-15	PE-15	PE-15 (1)	-
PE-16	DELIVERY AND REMOVAL	PE-16	PE-16	PE-16	-
PE-17	ALTERNATE WORK SITE		PE-17	PE-17	-
PE-18	LOCATION OF SYSTEM COMPONENTS			PE-18	-
PL-1	POLICY AND PROCEDURES	PL-1	PL-1	PL-1	-
PL-2	SYSTEM SECURITY AND PRIVACY PLANS	PL-2	PL-2	PL-2	-
PL-4	RULES OF BEHAVIOR	PL-4 (1)	PL-4 (1)	PL-4 (1)	-
PL-8	SECURITY AND PRIVACY ARCHITECTURES		PL-8	PL-8	-
PL-10	BASELINE SELECTION	PL-10	PL-10	PL-10	-
PL-11	BASELINE TAILORING	PL-11	PL-11	PL-11	-
PS-1	POLICY AND PROCEDURES	PS-1	PS-1	PS-1	-
PS-2	POSITION RISK DESIGNATION	PS-2	PS-2	PS-2	-
PS-3	PERSONNEL SCREENING	PS-3	PS-3	PS-3	-
PS-4	PERSONNEL TERMINATION	PS-4	PS-4	PS-4 (2)	-
PS-5	PERSONNEL TRANSFER	PS-5	PS-5	PS-5	-
PS-6	ACCESS AGREEMENTS	PS-6	PS-6	PS-6	-
PS-7	EXTERNAL PERSONNEL SECURITY	PS-7	PS-7	PS-7	-
PS-8	PERSONNEL SANCTIONS	PS-8	PS-8	PS-8	-
PS-9	POSITION DESCRIPTIONS	PS-9	PS-9	PS-9	-
RA-1	POLICY AND PROCEDURES	RA-1	RA-1	RA-1	-
RA-2	SECURITY CATEGORIZATION	RA-2	RA-2	RA-2	-
RA-3	RISK ASSESSMENT	RA-3 (1)	RA-3 (1)	RA-3 (1)	-
RA-5	VULNERABILITY MONITORING AND SCANNING	RA-5 (2) (11)	RA-5 (2) (5) (11)	RA-5 (2) (4) (5) (11)	-
RA-7	RISK RESPONSE	RA-7	RA-7	RA-7	-
RA-9	CRITICALITY ANALYSIS		RA-9	RA-9	-
SA-1	POLICY AND PROCEDURES	SA-1	SA-1	SA-1	-
SA-2	ALLOCATION OF RESOURCES	SA-2	SA-2	SA-2	The whole code is available on GitHub
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3	SA-3	SA-3	-
SA-4	ACQUISITION PROCESS	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (5) (9) (10)	-

SA-5	SYSTEM DOCUMENTATION	SA-5	SA-5	SA-5	System documentation is under README. md file that is together with the application in GitHub repository
SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	SA-8	SA-8	SA-8	-
SA-9	EXTERNAL SYSTEM SERVICES	SA-9	SA-9 (2)	SA-9 (2)	-
SA-10	DEVELOPER CONFIGURATION MANAGEMENT		SA-10	SA-10	All of the necessary configurations that are publicly available are in settings.py file
SA-11	DEVELOPER TESTING AND EVALUATION		SA-11	SA-11	-
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS		SA-15 (3)	SA-15 (3)	-
SA-16	DEVELOPER-PROVIDED TRAINING			SA-16	-
SA-17	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN			SA-17	-
SA-21	DEVELOPER SCREENING			SA-21	-
SA-22	UNSUPPORTED SYSTEM COMPONENTS	SA-22	SA-22	SA-22	-
SC-1	POLICY AND PROCEDURES	SC-1	SC-1	SC-1	-
SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY		SC-2	SC-2	-
SC-3	SECURITY FUNCTION ISOLATION			SC-3	-
SC-4	INFORMATION IN SHARED SYSTEM RESOURCES		SC-4	SC-4	-
SC-5	DENIAL-OF-SERVICE PROTECTION	SC-5	SC-5	SC-5	-
SC-7	BOUNDARY PROTECTION	SC-7	SC-7 (3) (4) (5) (7) (8)	SC-7 (3) (4) (5) (7) (8) (18) (21)	-
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY		SC-8 (1)	SC-8 (1)	-
SC-10	NETWORK DISCONNECT		SC-10	SC-10	When network disconnection occurs, the application is unavailable to use
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-12	SC-12	SC-12 (1)	Keys are managed by the admin
SC-13	CRYPTOGRAPHIC PROTECTION	SC-13	SC-13	SC-13	Database is protected by Private Key that is gnereated to the developer at the beginning of the application creation
SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS	SC-15	SC-15	SC-15	-
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES		SC-17	SC-17	-
SC-18	MOBILE CODE		SC-18	SC-18	-
SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOUR	SC-20	SC-20	SC-20	-
SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHI	SC-21	SC-21	SC-21	-
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION S	SC-22	SC-22	SC-22	-
SC-23	SESSION AUTHENTICITY		SC-23	SC-23	-
SC-24	FAIL IN KNOWN STATE			SC-24	-
SC-28	PROTECTION OF INFORMATION AT REST		SC-28 (1)	SC-28 (1)	-
SC-39	PROCESS ISOLATION	SC-39	SC-39	SC-39	-
SI-1	POLICY AND PROCEDURES	SI-1	SI-1	SI-1	-
SI-2	FLAW REMEDIATION	SI-2	SI-2 (2)	SI-2 (2)	-
SI-3	MALICIOUS CODE PROTECTION	SI-3	SI-3	SI-3	-
SI-4	SYSTEM MONITORING	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5) (10) (12) (14) (20) (22)	-
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-5	SI-5	SI-5 (1)	-
SI-6	SECURITY AND PRIVACY FUNCTION VERIFICATION			SI-6	-
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY		SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (15)	-
SI-8	SPAM PROTECTION		SI-8 (2)	SI-8 (2)	-

SI-10	INFORMATION INPUT VALIDATION		SI-10	SI-10	Input validation is performed when user is entering username and password. If one of the required fields is not given, then information pops up. Also if the password is to short or to easy to guess, a proper information is displayed to the user
SI-11	ERROR HANDLING		SI-11	SI-11	Errors occured when the admin could delete the room that is not in the database. It was solved by hadnling an exception
SI-12	INFORMATION MANAGEMENT AND RETENTION	SI-12	SI-12	SI-12	-
SI-16	MEMORY PROTECTION		SI-16	SI-16	Memory is protected by Private Key which is generated by Django when the application is created