	Risikovurdering									Risikohåndtering						
ID	Risiko - Hvad kan påvirke fortrolighed, tilgængelighed eller integritet?	Risikoejer	Hvorfor er dette en trussel/risiko?	Skøn for Konsekvens	Hvorfor vurderes Konsekvensen til dette?	Skøn for Sansynlighed	Hvorfor vurderes sandsynligheden til dette?	Beregnet risiko	Accepteret	Nye foranstaltninger	Konsekvens efter nye foranstaltninger	Ny sansynlighed	Ny restrisiko	Restrisiko Accepteret	Konklusion	Risikovillighed	Forklaring
1	Brugerne deler password		Fordi dette kan betyde at integriteten i systemet er væk	2	Fordi der kan potentielt ødelægges meget info	4	Fordi fokus er på at hjælpe borgeren og ikke om sikkerheden er okay	8					0			Grøn	
2	DDoS angreb	Serverdrift	Fordi det kan lægge hele servicen ned.	3	Hele servicen lægges ned	1	aau-giraf er meget ukendt.	3					0			1	Ledelsens vurdering af laveste risikoscore som er GRØN
3								0					0			Gul	
4	Default password står på hjemmesiden	Udviklere	Fordi alle der læser dokumentationen har superuseradgang på endpointet	3	Fordi en superuser kan ændre rigtig meget data	4	Det står i dokumentationen, i software og på hjemmesiden https://giraf.cs.aau.dk/	12					0			6	Ledelsens vurdering af laveste risikoscore som er GUL
5	At en bruger sletter data?		Fordi der er tvivl om der bliver lavet backup af databasen	4	Vi kan miste alt data	4	Fordi alle kan komme til at miste data	16					0			Rød	
6	At udviklerne tager en kopi af dataen ned til udvikling		Fordi det kan påvirke fortrolighed	2	Fordi indtil nu er det kun brugernes ugeplan	5	Udviklerne har direkte adgang og skal nogle gange teste	10					0				
7	Brugerne kan have svage passwords		Fordi det kan være for nemt at gætte passwords	3	Med et nemt password, kan en ond bruger logge ind	5	Fordi mange laver standard passwords	15					0			10	Ledelsens vurdering af laveste risikoscore som er RØD
8	Udviklerne efterlader passwords i clear text eller papir ved arbejdstationen		Fordi udviklerne skal have noget at teste med	4	Potentiale for at ødelægge meget	1	Udviklerne har egne udviklingsmiljøer	4					0				
9	En ond bruger får adgang til en andens weekplan.		Fordi brugerne så ikke kan genskabe deres data nemt.	2	De kan færdiggøre aktiviteter for andre brugere.	4	Hvis en guardian vælger den forkerte citizen	8					0				
10	En ond bruger får adgang til databasen og tager en kopi		Brud på fortrolighed, andre har adgang til privat information	5	Alt information relateret til brugere er nu i hænderne på andre der potentielt kan misbruge dataen. Det eneste om er beskyttet herunder er passwords.	1	Databasen er beskyttet af ITS	5					0				
11								0					0				
12								0					0				
13	En guardian efterlader en enhed logget ind		Andre kan bruge enheden til at på adgang til andres weekplan	3	Kan betyde at borgernes data bliver ændret/slettet.	4	Guardians har travlt og ikke altid tid til at logge ud.	12					0				
14	En developer kommer til at slette databasen		Dette er både tab på fortrolighed og integritet.	4	Hvis der ikke er taget backup inden for en rimelig tid kan der være mistet meget information eller planlægning	2	Giraf har mange nye hænder på projektet i starten	8					0				
15								0					0				
16								0					0				

17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0
29	0	0
30	0	0
31	0	0
32	0	0
33	0	0
34	0	0
35	0	0
36	0	0
37	0	0
38	0	0
39	0	0
40	0	0
41	0	0
42	0	0
43	0	0
44	0	0
45	0	0
46	0	0

47	0	0
48	0	0
49	0	0
50	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0