Artikel 1: Beperking

1.1

Infrastructuur- en/of informatiesystemen van BIT die geen onderdeel zijn van de beveiligingstest en infrastructuur- en/of informatiesystemen van andere cliënten van BIT, zullen niet worden gebruikt als opstapje voor toegang tot de systemen die deel uitmaken van de beveiligingstest.

1.2

Auditor zal alle redelijke inspanningen leveren om af te zien van activiteiten die de vertrouwelijkheid, integriteit of beschikbaarheid van informatiesystemen van BIT of andere cliënten van BIT in gevaar brengen (d.w.z. DDoS-aanvallen). Hoewel Auditor alle activiteiten in de beveiligingstest naar beste kunnen zal uitvoeren, kunnen de gebruikte hulpmiddelen en technieken de informatiesystemen van BIT verstoren en/of leiden tot mogelijk verlies of beschadiging van gegevens en BIT stemt ermee in om de nodige back-ups te maken en redundante systemen te bieden die vereist zijn in de omstandigheden. Auditor zal BIT op de hoogte stellen in het geval wanneer een activiteit leidt tot het uitvallen van de dienst of het verloren gaan van gegevens indien dit bekend is bij Auditor.

1.3

In het geval dat de activiteiten van de beveiligingstest de vertrouwelijkheid, integriteit of beschikbaarheid van de informatiesystemen van BIT of van andere cliënten van BIT in gevaar brengen, kan BIT de Auditor en/of Cliënt verzoeken de beveiligingstest onmiddellijk te stoppen.

1.4

BIT kan, zonder voorafgaand overleg met Auditor en/of Cliënt, acties ondernemen die de beveiligingstest hinderen of stilleggen in geval van beperking van de vertrouwelijkheid, integriteit of beschikbaarheid van de informatiesystemen van BIT of andere cliënten van BIT.

Artikel 2: Toestemming en vrijwaring

2.1

Omdat toegang verkrijgen tot een computersysteem zonder toestemming een misdrijf is volgens de Nederlandse wetgeving, geeft BIT expliciet toestemming aan Auditor om de overeengekomen activiteiten voor Cliënt uit te voeren.

2.2

Omdat het uitvoeren van de activiteiten in de beveiligingstest voor Cliënt mogelijk indruist tegen de Acceptable Use Policy van BIT, verklaart BIT dat de Acceptable Use Policy en de Abuse Policy niet van toepassing zijn op de activiteiten in de beveiligingstest gedurende het tijdsbestek zoals beschreven in artikel 16.

2.3

De Service Level Agreement(s) die BIT aanbiedt aan Cliënt zijn niet van toepassing tijdens de beveiligingstest of als gevolg van de beveiligingstest.

2.4

BIT vrijwaart Auditor voor claims van BIT, de cliënten van BIT en derden die verbonden zijn met BIT en/of cliënten van BIT – zowel voor directe als indirecte (vervolg)schade – die als gevolg zijn van de beveiligingstest of verband houden met de activiteiten van de beveiligingstest. Dit artikel is niet van toepassing in geval van grove nalatigheid, opzet of niet-naleving van de bepalingen van deze overeenkomst door Auditor.

Artikel 3: Data inbreuk

3.1

ndien tijdens de activiteiten van de beveiligingstest de gegevens van BIT, cliënten van BIT of een derde partij toegankelijk worden voor de Auditor, zal Auditor zijn toegang tot deze gegevens beperken voor zo ver dit mogelijk is binnen de activiteiten van de beveiligingstest.

3.2

Auditor verwijdert alle kopieën van de gegevens zoals beschreven in artikel 3.1 onmiddellijk na het voltooien van de activiteiten van de beveiligingstest.

Artikel 4: Informatie delen

4.1

Auditor deelt met BIT de kwetsbaarheden die op de infrastructuur van BIT en/of de informatiesystemen van BIT en/of de informatiesystemen van cliënten van BIT gevonden worden tijdens het uitvoeren van de activiteiten van de beveiligingstest.

4.2

Voor het type beveiligingstesten/-aanvallen die niet kunnen worden uitgevoerd vanwege beperkingen die door BIT zijn opgelegd, kan BIT, op verzoek, Auditor/Cliënt informeren over preventieve/beperkende maatregelen die BIT heeft getroffen om dit soort aanvallen te voorkomen (bijv. DDoS-aanvallen).

Artikel 5: Contact

5.1

Cliënt zal BIT informeren over de systemen en/of applicaties die deel uitmaken van de beveiligingstest en het tijdsbestek waarin de activiteiten van de beveiligingstest zullen worden uitgevoerd.

5.2

Auditor zal BIT informeren over de IP-adressen die hij zal gebruiken om de activiteiten van de beveiligingstest uit te voeren.

5.3

Auditor en Cliënt zullen BIT informeren over namen, telefoonnummer en e-mailadressen van directe contactpersonen of afdelingen binnen hun organisatie met betrekking tot de activiteiten van de beveiligingstest.

5.4

Het e-mailadres van de klantenservice van BIT is info@bit.nl. Gebruik cert@bit.nl met PGP KeyID 9DCA4A97A80E77B1 voor alle informatie die geheim moet blijven. Voor noodgevallen is BIT alleen telefonisch bereikbaar, 24x7 op 0318 648 688.

Artikel 6: Vertrouwelijkheid

6.1

Alle informatie en gegevens die uitgewisseld worden tussen Auditor, Cliënt en BIT, of informatie die bekend wordt, inclusief maar niet beperkt tot software, voorbereidingsmateriaal, documentatie, kennis of bedrijfsgeheimen van Auditor, Cliënt en BIT, zullen als vertrouwelijk behandeld worden door alle partijen. De ontvangende partij zal deze informatie alleen voor het beoogde doel gebruiken en niet delen met derden, behalve na schriftelijke toestemming of in geval van een wettelijke verplichting. BIT kan informatie over kwetsbaarheden die zijn gevonden op informatiesystemen van cliënten van BIT delen met de cliënt in kwestie.