Selbsterklärung zu den Anforderungen des Labels cyber-safe.ch

Name der antragstellenden Organisation:

Name des Dienstleisters:

Anleitung zur Selbstdeklaration:

Einige der folgenden Anforderungen können von Leistungen abhängen, die Sie für eine Organisation erbringen, die sich um das Label bewirbt; in diesem Fall geben Sie bitte an, ob die Dienstleistung die entsprechenden Anforderungen erfüllt.

In anderen Fällen kann die Anforderung ausserhalb Ihres Mandats liegen und daher nicht zutreffen (NZ); wenn Sie die Dienstleistung erbringen können, diese aber nicht im Leistungskatalog der antragstellenden Organisation enthalten ist, können Sie das Kästchen trifft nicht zu ankreuzen (NZ (optional).

Darüber hinaus finden Sie hier einige allgemeine Informationen über Ihre Organisation, die Sie uns bitte beantworten:

Haben Sie eine Richtlinie zur Informationssicherheit?	☐ Ja	☐ Nein
Haben Ihre Mitarbeiter ein Dokument mit den Rechten und Pflichten in Bezug auf IT-Ressourcen unterzeichnet?	☐ Ja	☐ Nein
Haben Sie bereits eine Kampagne zur Sensibilisierung für Phishing durchgeführt?	☐ Ja	☐ Nein
Haben Sie bereits einmal einen Schwachstellen-Scan Ihrer IT-Infrastruktur durchgeführt?	☐ Ja	☐ Nein
Bei Hosting, evtl. Tier-Klasse des Rechenzentrums?		
Haben Sie Zertifizierungen (Typ ISO, ITIL, ITSM, ISAE usw.) Wenn ja, welche:		

Anforderungen im Zusammenhang mit den Dienstleistungen, die für die antragstellende Organisation erbracht sind:

1 Bestand

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) Ein umfassendes Bestandsverzeichnis der ICT-Infrastruktur und aller mit dem/den geschäftlichen Netz(en) verbundenen Elemente der antragstellenden Organisation (Computer, Smartphone, Tablet, Internetobjekt usw.) ist vorhanden.	☐	☐	☐	☐
b) Ein umfassendes Bestandsverzeichnis der Cloud-Dienste mit Daten der antragstellenden Organisation ist vorhanden.	☐	☐	☐	☐

2 Verschlüsselung

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) Externe Kommunikationskanäle der antragstellenden Organisation (inkl. VPN) werden verschlüsselt.	☐	☐	☐	☐
b) Es ist zu ermitteln, welche Daten der antragstellenden Organisation verschlüsselt werden müssen (während der Übertragung und/oder Speicherung), und sicherzustellen, dass diese auch tatsächlich verschlüsselt werden.	☐	☐	☐	☐
c) Daten auf mobilen Geräten der antragstellenden Organisation (Computer, Smartphone, Tablet, Internetobjekt usw.) werden systematisch verschlüsselt.	☐	☐	☐	☐

3 WiFi der antragstellenden Organisation

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) WiFi-Netzwerke müssen verschlüsselt (min. WPA2) und durch ein Passwort geschützt sein*. (min. 16 Zeichen).	☐	☐	☐	☐
b) Das WiFi-Netz für Gäste muss vom geschäftlichen Netz getrennt sein.	☐	☐	☐	☐
c) Das interne WiFi-Netzwerk muss vom geschäftlichen Netz getrennt sein, wenn Mitarbeiter sich mit nicht im Bestandsverzeichnis aufgeführten Geräten verbinden, können (z. B. Smartphones, private Geräte usw.), die das geschäftliche Netz unter keinen Umstanden nutzen dürfen.	☐	☐	☐	☐

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
d) Es muss ein logisches Netzwerk (VLAN) für IP-Telefone (IP- Phones) eingerichtet sein, das vom geschäftlichen Netz getrennt ist.	☐	☐	☐	☐

* bei dem es sich nicht um das Standardpasswort handeln darf.

4 Physischer Zugang

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) Sämtliche Anlagen, in denen Daten der antragstellenden Organisation untergebracht sind, müssen gegen physischen Zugriff durch Unbefugte geschützt sein.	☐	☐	☐	☐
b) Der Zugriff auf das Rechenzentrum der antragstellenden Organisation durch externe Personen wird kontrolliert (z. B. Liste mit Angaben zu den Personen, die das Rechenzentrum betreten, Uhrzeit, von welchem Lieferanten usw.).	☐	☐	☐	☐
c) Nicht mehr benutzte Datenträger der antragstellenden Organisation werden so entsorgt, dass die darauf enthaltenen Daten dauerhaft vernichtet werden.	☐	☐	☐	☐

5 Personal Abteilung

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) Die antragstellende Organisation muss eine aktuelle Liste der Zugriffsberechtigungen für alle Datenkategorien und Arten von Mitarbeitenden fuhren (Berechtigungsplan).	☐	☐	☐	☐
b) Die antragstellende Organisation muss mindestens einmal jährlich überprüfen, ob die Liste der Zugangsberechtigungen den tatsächlich gewährten Rechten entspricht.	☐	☐	☐	☐
c) Kein Mitarbeitender der antragstellenden Organisation darf an seinem lokalen Arbeitsplatz über Administratorenrechte verfügen, mit Ausnahme von IT-Mitarbeitern.	☐	☐	☐	☐

6 Verfahren, Routinen

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) Updates für die Betriebssysteme der Geräte und Server der antragstellenden Organisation werden angewendet und regelmäßig überprüft.	☐	☐	☐	☐
b) Softwareprogramme (ausser Geschäftssoftware) von Geräten und Servern der antragstellenden Organisation werden angewendet und regelmäßig überprüft.	☐	☐	☐	☐
c) Die Netzwerkausstattung der antragstellenden Organisation wird regelmässig aktualisiert.	☐	☐	☐	☐
d) Auf allen Geräten der antragstellenden Organisation wird regelmässig überprüft, ob ein Antivirusprogramm vorhanden ist, das zudem regelmässig aktualisiert wird.	☐	☐	☐	☐
e) Sicherheitswarnungen der antragstellenden Organisation werden zentralisiert und regelmässig verarbeitet.	☐	☐	☐	☐
f) Zwischen dem geschäftlichen Netz und dem externen Netz der antragstellenden Organisation besteht eine Firewall.	☐	☐	☐	☐
g) Die Funktion, Konfiguration und Aktualisierung der Firewall der antragstellenden Organisation wird regelmässig überprüft.	☐	☐	☐	☐

7 Sicherung

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) Die antragstellende Organisation muss über ein Datensicherungssystem verfügen.	☐	☐	☐	☐
b) Die Sicherung wird mindestens einmal pro Woche durchgeführt.	☐	☐	☐	☐
c) Die Sicherung wird mindestens einmal pro Tag durchgeführt.	☐	☐	☐	☐
d) Die antragstellende Organisation muss in der Lage sein, den Status ihres Systems und ihrer Daten wieder auf den Status von vor einem Monat zurückzusetzen.	☐	☐	☐	☐
e) Die antragstellende Organisation muss in der Lage sein, den Status ihres Systems und ihrer Daten wieder auf den Status von vor drei Monaten zurückzusetzen.	☐	☐	☐	☐

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
f) Die antragstellende Organisation muss in der Lage sein, den Status ihres Systems und ihrer Daten wieder auf den Status von vor sechs Monaten zurückzusetzen.	☐	☐	☐	☐
g) Die ordnungsgemässe Funktion der Sicherung wird mindestens einmal pro Woche überprüft.	☐	☐	☐	☐
h) Eine Kopie der Daten befindet sich an einem zweiten Standort, der mindestens 10 km entfernt ist.	☐	☐	☐	☐
i) Es ist nicht möglich, dass eine Person (einschliesslich des Administrators) alle Sicherungsdaten löschen kann.	☐	☐	☐	☐
j) Ein Test zur Wiederherstellung der neusten und ältesten Sicherungsdaten muss mindestens einmal pro Jahr durchgeführt werden.	☐	☐	☐	☐

8 Resilienz

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) Es gibt einen Plan bzw. Verfahren für die Wiederherstellung im Falle einer Unterbrechung der IT-Produktion der antragstellenden Organisation.	☐	☐	☐	☐
b) Die Verfahren für die Wiederherstellung werden mindestens einmal pro Jahr getestet bei der antragstellenden Organisation.	☐	☐	☐	☐

9 Passwörter

Passwortrichtlinien müssen so implementiert werden, dass jeder Mitarbeitender zu ihrer Einhaltung verpflichtet ist.

Anforderung	NZ	NZ (option)	Bestätig	Nicht bestätigt
a) Passwörter der antragstellenden Organisation müssen aus mindestens 10 Zeichen bestehen und Gross- und Kleinbuchstaben, Zahlen sowie Sonderzeichen enthalten.	☐	☐	☐	☐

Ort und Datum:

Unterschrift des Dienstleisters:

Beispiel für eine begleitende Nachricht

Sehr geehrter Herr, sehr geehrte Frau,

Diese Nachricht wird Ihnen im Rahmen des Prozesses zur Zertifizierung unserer Organisation nach den Anforderungen des Labels cyber-safe.ch zugesandt.
Als IT-Dienstleister hängt verschiedene Anforderungen des Labels von den Leistungen ab, die Sie für uns erbringen. Aus diesem Grund finden Sie im Anhang ein Formular zur Selbstdeklaration, welches wir Sie bitten, auszufüllen und uns unterschrieben zurückzusenden. Dies wird uns ermöglichen, eine gewisse Anzahl von Anforderungen des Labels zu validieren und den Leistungskatalog, den wir bei Ihrer Organisation haben, besser zu dokumentieren.

Wir danken Ihnen für die Aufmerksamkeit, und wünschen Ihnen einen schönen Tag.

Freundliche Grüsse,