Richtlinien

gemäß § 2a Nr. 4 Fraktionsgesetz über die Inanspruchnahme von Dienstleistungen und die Nutzung technischer Einrichtungen der Bürgerschaftskanzlei durch die Fraktionen und Gruppen sowie die unentgeltliche Überlassung von Räumen und Gegenständen an die Fraktionen und Gruppen

I. Inanspruchnahme von Dienstleistungen und Nutzung technischer Einrichtungen der Bürgerschaftskanzlei nach § 2a Nr. 1 des Fraktionsgesetzes

1. Die Fraktionen und Gruppen können die von der Bürgerschaftskanzlei erbrachten Dienstleistungen unentgeltlich in Anspruch nehmen. Es handelt sich dabei im Wesentlichen um folgende Dienstleistungen:
   a. Fachliche und rechtliche Beratung in parlamentarischen Fragen.
   b. Bereitstellung von Materialien an die Fraktionen und Gruppen zur Koordinierung ihrer Arbeit, zur Information ihrer Mitarbeiterinnen und Mitarbeiter bzw. als Unterstützung ihrer Öffentlichkeitsarbeit, wie z.B. täglicher Pressespiegel, Broschüren, Informationsmaterial, Sitzungskalender oder Einladungen zu Veranstaltungen der Bürgerschaft.
   c. Bereitstellung von Materialien, die die parlamentarischen Abläufe betreffen, wie z.B. Drucksachen, Tagesordnungen, Plenar- und Ausschussprotokolle, Wochenübersichten etc.
   d. Durchführung von themen- und personenbezogenen Recherchen in internen und externen Datenbanken, Bereitstellung von Informationen und Fundstellenlisten zu parlamentarischen Abläufen und Gesetzen der Länder und des Bundes.
   e. Bereitstellung von Literatur und Medien.
   f. Verwaltungstätigkeit im Zusammenhang mit der Ausgabe und Abrechnung von Fahrkarten des HVV sowie mit der Anmietung von Räumlichkeiten für die Fraktionen und Gruppen außerhalb des Rathauses.
   g. Beratung und Koordinierung zur Sicherstellung des IT-Betriebes sowie der Einhaltung von Sicherheitsrichtlinien und Standards.
   h. Inbetriebnahme der IT-Infrastruktur sowie deren Betreuung als „Second Level Support".

2. Die Fraktionen und Gruppen können die technischen Einrichtungen der Bürgerschaftskanzlei nutzen. Dazu zählen:
   a. die vorhandene Netzwerk- und Serverinfrastruktur, das Intranet, das WLAN sowie
   b. im Rahmen der vorhandenen Kapazitäten und unter Berücksichtigung der Belange der Bürgerschaftskanzlei die Kopierer im Rathaus und in den übrigen Dienstgebäuden. Die mit der Nutzung der Kopierer verbundenen Kosten sind zu erstatten.

II. Unentgeltliche Überlassung von Räumen und Gegenständen an die Fraktionen und Gruppen nach § 2a Nr. 2 des Fraktionsgesetzes

1. Den Fraktionen und Gruppen werden zur Erledigung ihrer Aufgaben unter Berücksichtigung eines Grundbedarfs sowie ihrer Stärke angemessene Räume im Rathaus sowie in anderen Gebäuden überlassen. Die Räume werden entweder durch die Bürgerschaftskanzlei oder durch die Fraktion oder Gruppe angemietet. Im letzteren Fall werden die angemessenen Miet- und Nebenkosten einschließlich der Maklercourtage durch die Bürgerschaftskanzlei erstattet. Für die Ermittlung der Fläche der den Fraktionen jeweils zustehenden Räume sowie die Modalitäten der Berechnung ist die als **Anlage 1** beigefügte Tabelle maßgeblich. Die im Rathaus überlassenen Räume werden lediglich ihrer Funktion nach angerechnet. Die Höhe des Richtwertes für die Quadratmeter-Miete orientiert sich an den für die Innenstadt erhobenen Durchschnittswerten der Firma Grossmann und Berger und wird mit Beginn jeder Wahlperiode überprüft.
   In Anbetracht der zentralen Lage des Rathauses, das durch die Fraktionen jederzeit mit zumutbarem Aufwand erreichbar sein muss, ist bei der Anmietung von Bestandsimmobilien mit Abweichungen zu den in der Anlage 1 beschriebenen Richtwerten zu rechnen. Eine wirtschaftlich vertretbare und an die tatsächlichen Gegebenheiten angepasste Lösung ist anzustreben.

2. Die unentgeltliche Überlassung umfasst auch die Übernahme der Nebenkosten, angelehnt an die Betriebskostenverordnung - BetrKV - (siehe **Anlage 2**), wie z. B. für Heizung, Strom, Wasser.

3. Für Sitzungen und sonstige Veranstaltungen der Fraktionen und Gruppen im Rathaus und im Dienstgebäude Schmiedestraße werden Sitzungsräume im Rahmen der vorhandenen Kapazitäten zur Verfügung gestellt. Eine Nutzung des Plenarsaals ist ausgeschlossen.

4. Für die Arbeitsplätze der Fraktionen und Gruppen werden eine einheitliche IT-Ausstattung sowie Telefone (ggf. mit Gruppenfunktion) und Faxanschlüsse unentgeltlich bereitgestellt. Ausnahmen von dieser Grundausstattung oder Erweiterungen können im Einzelfall zur Verfügung gestellt werden. In diesem Fall sind die Mehrkosten von den Fraktionen und Gruppen zu tragen. Betriebsmittel für Drucker, Datenträger u. Ä. werden nicht erstattet. Die Anzahl der bereitgestellten IT-Arbeitsplatzausstattungen orientiert sich an der Zahl der unter Ziffer II 1 zur Verfügung gestellten Räume und wird in der **Anlage 3** zu diesen Richtlinien dokumentiert.
   Die Modalitäten für die Bereitstellung der IT-Infrastruktur sowie für die damit verbundenen Dienstleistungen (Ziff. I 1 g-h) werden in einer gesonderten Anlage zu diesen Richtlinien beschrieben (**Anlage 3** zu den Richtlinien zum Fraktionsgesetz).

5. Den Fraktionen und Gruppen wird je ein Kopier-/Drucksystem (ohne Betriebsmittel) zur Verfügung gestellt.

III. Nutzung von Dienstkraftfahrzeugen mit Fahrerin oder Fahrer durch die Vorsitzenden der Fraktionen und Gruppen nach § 2a Nr. 3 i. V. m. § 6 Abs. 3 des Fraktionsgesetzes

1. Die Inanspruchnahme von Dienstkraftfahrzeugen für Fahrten zwischen Wohnung und Arbeitsstätte, dienstliche und private Fahrten richtet sich nach den für Senatorinnen bzw. Senatoren und Staatsrätinnen bzw. Staatsräte geltenden Bestimmungen.
2. Die Bürgerschaftskanzlei erstellt den Vorsitzenden der Fraktionen und Gruppen jährlich nach Ablauf eines Kalenderjahres nach den jeweils geltenden steuerrechtlichen Bestimmungen eine Bescheinigung über den geldwerten Vorteil, der aus der unentgeltlichen Überlassung eines Dienstfahrzeuges entsteht, zur Vorlage beim Finanzamt zur Mitversteuerung. Die Vorsitzenden der Fraktionen und Gruppen haben die Wahl zwischen einer pauschalen und einer individuellen Nutzwertermittlung.
3. Die Nutzerinnen und Nutzer haben die für die Berechnung notwendigen Daten der Bürgerschaftskanzlei zu übermitteln, sofern diese nicht bereits der Bürgerschaftskanzlei vorliegen.
4. Für Zeiten der Inanspruchnahme des geldwerten Äquivalents nach § 2a Ziffer 3 Satz 1 des Fraktionsgesetzes treten die Fraktionen an die Stelle der Bürgerschaftskanzlei hinsichtlich der Aufgaben nach III. Nr. 2 und 3 dieser Richtlinien.

IV. Weitere Vereinbarungen

Nach Inkrafttreten dieser Richtlinie besteht die Möglichkeit, diese durch Anlagen zu ergänzen, um weitere, insbesondere noch für den IT-Bereich erforderliche Konkretisierungen vorzunehmen. Gültig ist jeweils die aktuellste Fassung einer Anlage, die inhaltlich zwischen den Fraktionen und der Bürgerschaftskanzlei abgestimmt und von der Präsidentin erlassen worden ist.

V. Aufhebung der bisherigen Richtlinien

Diese Richtlinien treten mit Wirkung vom 01. März 2018 an die Stelle der bisherigen Richtlinien vom 06. März 2012.

Hamburg, den 27. Februar 2018

Carola Veit
Präsidentin der Hamburgischen Bürgerschaft

Raumbezeichnung	Bemerkung	Bedarf	Raumgröße	Fraktionsanspruch	Raumbedarf
Fraktionsvorsitz	Vorsitz	Grundbedarf	25	6	150,0
Fraktionsvorsitz	Stellvertretung	Grundbedarf	20	6	120,0
Geschäftsführung	Parlamentarische/r Geschäftsführe/r	Grundbedarf	20	6	120,0
Geschäftsführung	Fraktionsgeschäftsführer/-in	Grundbedarf	15	12	180,0
Pressestelle	Presse und Öffentlichkeitsarbeit	Grundbedarf	15	12	180,0
Öffentlichkeitsarbeit		Grundbedarf	15	6	90,0
Sekretariat des Fraktionsvorstandes	Sekretariat für 1 bis 2 Arbeitsplätze	Grundbedarf	15	6	90,0
Finanzbuchhaltung		Grundbedarf	15	6	90,0
PraktikantInnen, ReferendarInnen		Grundbedarf	15	6	90,0
Küche		Grundbedarf	10	6	60,0
WC	Getrennt nach Geschlechtern ist wünschenswert.	Grundbedarf	10	6	60,0
Technikraum	Raum für Server, Kopierer, Drucker o. ä.	Grundbedarf	15	6	90,0
Abstellaum/Archiv	Materiallager, Aktenlager, Hilfsmittellager o. ä.	Grundbedarf	15	6	90,0
Besprechungsraum	je Person	Grundbedarf	4	90	360,0
Arbeitsräume	Aufschlag für weitere Räume X m² je Fraktionsmitglied	Zusatzbedarf	13	45	585,0
Hauptflächen				**Gesamtbedarf:**	2.355,00
Nebenflächen	X% des Gesamtbedarfs	Grundbedarf	471,00	20%	471,00
Gesamt					2.826,00

Fraktion	Sitze	Deckelung
SPD	59	30
CDU	20	20
GRÜNE	14	14
LINKE	10	10
FDP	9	9
AfD	7	7
Summe	119	90

Gewichtung	0,5

Verordnung über die Aufstellung von Betriebskosten (Betriebskostenverordnung - BetrKV)

BetrKV

Ausfertigungsdatum: 25.11.2003

Vollzitat:

"Betriebskostenverordnung vom 25. November 2003 (BGBl. I S. 2346, 2347), die durch Artikel 4 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958) geändert worden ist"

Stand: Geändert durch Art. 4 G v. 3.5.2012 I 958

Fußnote

(+++ Textnachweis ab: 1. 1.2004 +++)

Die V wurde als Artikel 1 d. V v. 25.11.2003 I 2346 von der Bundesregierung und dem Bundesministerium für Familie, Senioren, Frauen und Jugend im Einvernehmen mit dem Bundesministerium für Wirtschaft und Arbeit, dem Bundesministerium für Verkehr, Bau- und Wohnungswesen und dem Bundesministerium für Gesundheit und Soziale Sicherung mit Zustimmung des Bundesrates verordnet. Sie ist gem. Art. 6 der V mWv 1.1.2004 in Kraft getreten.

§ 1 Betriebskosten

(1) Betriebskosten sind die Kosten, die dem Eigentümer oder Erbbauberechtigten durch das Eigentum oder Erbbaurecht am Grundstück oder durch den bestimmungsmäßigen Gebrauch des Gebäudes, der Nebengebäude, Anlagen, Einrichtungen und des Grundstücks laufend entstehen. Sach- und Arbeitsleistungen des Eigentümers oder Erbbauberechtigten dürfen mit dem Betrag angesetzt werden, der für eine gleichwertige Leistung eines Dritten, insbesondere eines Unternehmers, angesetzt werden könnte; die Umsatzsteuer des Dritten darf nicht angesetzt werden.

(2) Zu den Betriebskosten gehören nicht:

1. die Kosten der zur Verwaltung des Gebäudes erforderlichen Arbeitskräfte und Einrichtungen, die Kosten der Aufsicht, der Wert der vom Vermieter persönlich geleisteten Verwaltungsarbeit, die Kosten für die gesetzlichen oder freiwilligen Prüfungen des Jahresabschlusses und die Kosten für die Geschäftsführung (Verwaltungskosten),
2. die Kosten, die während der Nutzungsdauer zur Erhaltung des bestimmungsmäßigen Gebrauchs aufgewendet werden müssen, um die durch Abnutzung, Alterung und Witterungseinwirkung entstehenden baulichen oder sonstigen Mängel ordnungsgemäß zu beseitigen (Instandhaltungs- und Instandsetzungskosten).

§ 2 Aufstellung der Betriebskosten

Betriebskosten im Sinne von § 1 sind:

1. die laufenden öffentlichen Lasten des Grundstücks,
   hierzu gehört namentlich die Grundsteuer;
2. die Kosten der Wasserversorgung,
   hierzu gehören die Kosten des Wasserverbrauchs, die Grundgebühren, die Kosten der Anmietung oder anderer Arten der Gebrauchsüberlassung von Wasserzählern sowie die Kosten ihrer Verwendung einschließlich der Kosten der Eichung sowie der Kosten der Berechnung und Aufteilung, die Kosten der Wartung von Wassermengenreglern, die Kosten des Betriebs einer hauseigenen Wasserversorgungsanlage und einer Wasseraufbereitungsanlage einschließlich der Aufbereitungsstoffe;
3. die Kosten der Entwässerung,

hierzu gehören die Gebühren für die Haus- und Grundstücksentwässerung, die Kosten des Betriebs einer entsprechenden nicht öffentlichen Anlage und die Kosten des Betriebs einer Entwässerungspumpe;

4. die Kosten

   a) des Betriebs der zentralen Heizungsanlage einschließlich der Abgasanlage, hierzu gehören die Kosten der verbrauchten Brennstoffe und ihrer Lieferung, die Kosten des Betriebsstroms, die Kosten der Bedienung, Überwachung und Pflege der Anlage, der regelmäßigen Prüfung ihrer Betriebsbereitschaft und Betriebssicherheit einschließlich der Einstellung durch eine Fachkraft, der Reinigung der Anlage und des Betriebsraums, die Kosten der Messungen nach dem Bundes-Immissionsschutzgesetz, die Kosten der Anmietung oder anderer Arten der Gebrauchsüberlassung einer Ausstattung zur Verbrauchserfassung sowie die Kosten der Verwendung einer Ausstattung zur Verbrauchserfassung einschließlich der Kosten der Eichung sowie der Kosten der Berechnung und Aufteilung

   oder

   b) des Betriebs der zentralen Brennstoffversorgungsanlage,
   hierzu gehören die Kosten der verbrauchten Brennstoffe und ihrer Lieferung, die Kosten des Betriebsstroms und die Kosten der Überwachung sowie die Kosten der Reinigung der Anlage und des Betriebsraums

   oder

   c) der eigenständig gewerblichen Lieferung von Wärme, auch aus Anlagen im Sinne des Buchstabens a,
   hierzu gehören das Entgelt für die Wärmelieferung und die Kosten des Betriebs der zugehörigen Hausanlagen entsprechend Buchstabe a

   oder

   d) der Reinigung und Wartung von Etagenheizungen und Gaseinzelfeuerstätten,
   hierzu gehören die Kosten der Beseitigung von Wasserablagerungen und Verbrennungsrückständen in der Anlage, die Kosten der regelmäßigen Prüfung der Betriebsbereitschaft und Betriebssicherheit und der damit zusammenhängenden Einstellung durch eine Fachkraft sowie die Kosten der Messungen nach dem Bundes-Immissionsschutzgesetz;

5. die Kosten

   a) des Betriebs der zentralen Warmwasserversorgungsanlage,
   hierzu gehören die Kosten der Wasserversorgung entsprechend Nummer 2, soweit sie nicht dort bereits berücksichtigt sind, und die Kosten der Wassererwärmung entsprechend Nummer 4 Buchstabe a

   oder

   b) der eigenständig gewerblichen Lieferung von Warmwasser, auch aus Anlagen im Sinne des Buchstabens a,
   hierzu gehören das Entgelt für die Lieferung des Warmwassers und die Kosten des Betriebs der zugehörigen Hausanlagen entsprechend Nummer 4 Buchstabe a

   oder

   c) der Reinigung und Wartung von Warmwassergeräten,
   hierzu gehören die Kosten der Beseitigung von Wasserablagerungen und Verbrennungsrückständen im Innern der Geräte sowie die Kosten der regelmäßigen Prüfung der Betriebsbereitschaft und Betriebssicherheit und der damit zusammenhängenden Einstellung durch eine Fachkraft;

6. die Kosten verbundener Heizungs- und Warmwasserversorgungsanlagen

   a) bei zentralen Heizungsanlagen entsprechend Nummer 4 Buchstabe a und entsprechend Nummer 2, soweit sie nicht dort bereits berücksichtigt sind,

   oder

   b) bei der eigenständig gewerblichen Lieferung von Wärme entsprechend Nummer 4 Buchstabe c und entsprechend Nummer 2, soweit sie nicht dort bereits berücksichtigt sind,

   oder

   c) bei verbundenen Etagenheizungen und Warmwasserversorgungsanlagen entsprechend Nummer 4 Buchstabe d und entsprechend Nummer 2, soweit sie nicht dort bereits berücksichtigt sind;

7. die Kosten des Betriebs des Personen- oder Lastenaufzugs,

hierzu gehören die Kosten des Betriebsstroms, die Kosten der Beaufsichtigung, der Bedienung, Überwachung und Pflege der Anlage, der regelmäßigen Prüfung ihrer Betriebsbereitschaft und Betriebssicherheit einschließlich der Einstellung durch eine Fachkraft sowie die Kosten der Reinigung der Anlage;

8. die Kosten der Straßenreinigung und Müllbeseitigung,
zu den Kosten der Straßenreinigung gehören die für die öffentliche Straßenreinigung zu entrichtenden Gebühren und die Kosten entsprechender nicht öffentlicher Maßnahmen; zu den Kosten der Müllbeseitigung gehören namentlich die für die Müllabfuhr zu entrichtenden Gebühren, die Kosten entsprechender nicht öffentlicher Maßnahmen, die Kosten des Betriebs von Müllkompressoren, Müllschluckern, Müllabsauganlagen sowie des Betriebs von Müllmengenerfassungsanlagen einschließlich der Kosten der Berechnung und Aufteilung;

9. die Kosten der Gebäudereinigung und Ungezieferbekämpfung,
zu den Kosten der Gebäudereinigung gehören die Kosten für die Säuberung der von den Bewohnern gemeinsam genutzten Gebäudeteile, wie Zugänge, Flure, Treppen, Keller, Bodenräume, Waschküchen, Fahrkorb des Aufzugs;

10. die Kosten der Gartenpflege,
hierzu gehören die Kosten der Pflege gärtnerisch angelegter Flächen einschließlich der Erneuerung von Pflanzen und Gehölzen, der Pflege von Spielplätzen einschließlich der Erneuerung von Sand und der Pflege von Plätzen, Zugängen und Zufahrten, die dem nicht öffentlichen Verkehr dienen;

11. die Kosten der Beleuchtung,
hierzu gehören die Kosten des Stroms für die Außenbeleuchtung und die Beleuchtung der von den Bewohnern gemeinsam genutzten Gebäudeteile, wie Zugänge, Flure, Treppen, Keller, Bodenräume, Waschküchen;

12. die Kosten der Schornsteinreinigung,
hierzu gehören die Kehrgebühren nach der maßgebenden Gebührenordnung, soweit sie nicht bereits als Kosten nach Nummer 4 Buchstabe a berücksichtigt sind;

13. die Kosten der Sach- und Haftpflichtversicherung,
hierzu gehören namentlich die Kosten der Versicherung des Gebäudes gegen Feuer-, Sturm-, Wasser- sowie sonstige Elementarschäden, der Glasversicherung, der Haftpflichtversicherung für das Gebäude, den Öltank und den Aufzug;

14. die Kosten für den Hauswart,
hierzu gehören die Vergütung, die Sozialbeiträge und alle geldwerten Leistungen, die der Eigentümer oder Erbbauberechtigte dem Hauswart für seine Arbeit gewährt, soweit diese nicht die Instandhaltung, Instandsetzung, Erneuerung, Schönheitsreparaturen oder die Hausverwaltung betrifft; soweit Arbeiten vom Hauswart ausgeführt werden, dürfen Kosten für Arbeitsleistungen nach den Nummern 2 bis 10 und 16 nicht angesetzt werden;

15. die Kosten

    a) des Betriebs der Gemeinschafts-Antennenanlage,
    hierzu gehören die Kosten des Betriebsstroms und die Kosten der regelmäßigen Prüfung ihrer Betriebsbereitschaft einschließlich der Einstellung durch eine Fachkraft oder das Nutzungsentgelt für eine nicht zu dem Gebäude gehörende Antennenanlage sowie die Gebühren, die nach dem Urheberrechtsgesetz für die Kabelweitersendung entstehen,

    oder

    b) des Betriebs der mit einem Breitbandnetz verbundenen privaten Verteilanlage; hierzu gehören die Kosten entsprechend Buchstabe a, ferner die laufenden monatlichen Grundgebühren für Breitbandanschlüsse;

16. die Kosten des Betriebs der Einrichtungen für die Wäschepflege,
hierzu gehören die Kosten des Betriebsstroms, die Kosten der Überwachung, Pflege und Reinigung der Einrichtungen, der regelmäßigen Prüfung ihrer Betriebsbereitschaft und Betriebssicherheit sowie die Kosten der Wasserversorgung entsprechend Nummer 2, soweit sie nicht dort bereits berücksichtigt sind;

17. sonstige Betriebskosten,
hierzu gehören Betriebskosten im Sinne des § 1, die von den Nummern 1 bis 16 nicht erfasst sind.

Bürgerschaft der Freien und Hansestadt Hamburg
Bürgerschaftskanzlei

Anlage 3

zu den Richtlinien zum

Fraktionsgesetz

Version 1.04 vom 31.01.2018

Version	Datum	Änderungsgründe	Autor
0.1	08.04.2011	Dokumenterstellung	A2
0.2	19.04.2011	A2 intern abgestimmte Fassung	Referat A2
0.3	11.05.2011	Anmerkungen A	A (komm. V.)
0.4	17.05.2011	Anmerkungen u. Kenntnisnahme L	L
0.5	24.05.2011	Kenntnisnahme im Vorwege GAL- und SPD-Fraktion	
0.6	15.03.2012	Überarbeiteter Entwurf als Anlage 2 zu den Richtlinien zum FraktG.	A2
0.7	05.04.2012	Abstimmung mit A	A2, A
0.8	12.04.2012	Abstimmung C	C100, A, A2
0.9		Abstimmung u. Genehmigung L	
0.10	27.09.2012	Abstimmung IT-AG Fraktionen	SPD, FDP, CDU, Grüne
0.11	31.10.2012/ 14.11.2012	Änderungsvorschläge Grüne Frakt.	Grüne
1.0	06.12.2012/ 19.12.2012	Exemplar zur Schlussabstimmung und anschl. Unterzeichnung	A
1.01	01.09.2016	Änderungen in Ziff. 2,3; Anpassung der Links Anhang A	A2
1.02	05.12.2016	Bemessungsgrundlage für die PC-Ausstattung (Ziff. 7.1.1); Umbenennung in Anlage 3	A2
1.03	05.12.2016	Anmerkungen A	A (komm. V.)
1.04	31.01.2018/ 26.2.2018	Einarbeitung der Diskussionsergebnisse 2017 und grammatikalische Korrekturen	A2 und A

1) Gegenstand

(1) In dieser Anlage zu den Richtlinien zum Fraktionsgesetz (Fassung vom 1.3.2018) werden die IT-Ausstattung und der IT-Betrieb der Fraktionen und Gruppen in der Hamburgischen Bürgerschaft sowie die damit verbundenen Zuständigkeiten und Aufgaben weiter konkretisiert.

(2) Bestandteil dieser Anlage sind die Planung der Ausstattung, die Beschaffung, die Installation und der Betrieb von PC und Notebooks, Netzwerk und Servern, die Software-Ausstattung sowie die Anwendung und Einhaltung der Sicherheitsstandards.

(3) Nicht Gegenstand dieser Anlage sind die Bereitstellung von Telefonen, Faxgeräten, Druckern, Kopierern, Mobiltelefonen und Smartphones, WLAN-Infrastruktur oder sonstige, in den Richtlinien zum Fraktionsgesetz beschriebene Dienstleistungen.

(4) Da die IT einem schnellen und teilweise weitreichenden Wandel der Technologie, der Sicherheit und der Verfügbarkeits- bzw. Nutzungsanforderungen unterworfen ist, sind regelmäßige Überprüfungen der Angemessenheit und Aktualität der Regelungen notwendig und es können ggf. zusätzliche Vereinbarungen getroffen werden.

2) Zuständigkeiten

(1) Für IT-Ausstattung und -Betrieb nach den Richtlinien zum Fraktionsgesetz sowie für die Bereitstellung der entsprechenden IT-Infrastruktur ist die Bürgerschaftskanzlei zuständig. Teilleistungen (z.B. Outlook-Dienste und Netzzugänge) werden nach Beauftragung durch die Bürgerschaftskanzlei durch Dataport erbracht. Dabei hat die Bürgerschaftskanzlei sicherzustellen, dass die vertraglich vereinbarten Leistungen entsprechend erfüllt werden.

(2) Die Fraktionen benennen eine Keyuserin bzw. einen Keyuser sowie eine Vertreterin bzw. einen Vertreter für den First-Level-Support in der Fraktion. Die Keyuserinnen und Keyuser der Fraktionen sind neben den Fraktionsgeschäftsführer/-innen Ansprechpartnerinnen und Ansprechpartner für das IT-Referat der Bürgerschaftskanzlei in IT-Angelegenheiten.

(3) Die Fraktionen sind für die IT-Ausstattung, die nicht Bestandteil der Richtlinien zum Fraktionsgesetz ist, selbst zuständig. Sofern diese zusätzliche IT-Ausstattung Bestandteil des Netzes der Bürgerschaft bzw. des Datennetzes der FHH sein soll, sind die Beschaffung, Einrichtung und der Betrieb mit dem IT-Referat abzustimmen. Für diese Produkte oder Dienstleistungen, werden Bestellung und Auftragsabwicklung durch das IT-Referat der Bürgerschaftskanzlei im Einzelfall unterstützt. Rechnungsempfänger ist die beauftragende Fraktion. Nach einem Grundsatzvermerk der Finanzbehörde ist in diesem Fall die geltende Umsatzsteuer zu entrichten.

(4) Die Zuständigkeiten aller Beteiligten beinhalten die grundsätzliche Verpflichtung und Verantwortung zur Umsetzung der Vorgaben für die IT-Ausstattung und den Betrieb sowie für die Einhaltung der Datensicherheit und des Datenschutzes.

3) Beratung und Koordinierung

(1) Neben der Bereitstellung der für die Fraktionsarbeit benötigten IT-Infrastruktur steht das IT-Referat der Bürgerschaftskanzlei[1] den Fraktionen und Gruppen[2] als Ansprechpartner in sämtlichen IT-Angelegenheiten beratend zur Verfügung. Dies gilt auch für Vorhaben, die nicht in den Richtlinien zum Fraktionsgesetz enthalten sind.

(2) Jeweils zu Beginn einer Wahlperiode oder bei Bedarf wird eine IT-Koordinierungsgruppe berufen. Dieses Gremium setzt sich zusammen aus Vertreterinnen und Vertretern der Fraktionen, Abgeordneten sowie aus Vertreterinnen und Vertretern der Bürgerschaftskanzlei. Dieses Gremium berät über künftige IT-Vorhaben und Entwicklungen und erarbeitet Entscheidungsempfehlungen für deren Umsetzung. Das IT-Referat lädt die Keyuserinnen und

[1] im Folgenden: IT-Referat

[2] im Folgenden: Fraktion bzw. Fraktionen

Keyuser der Fraktionen zweimal jährlich zu einem Informationstreffen und zu einem Meinungsaustausch ein. In diesem Treffen berichtet das IT-Referat über aktuelle Entwicklungen und bietet ein Forum zur Erörterung der IT-Angelegenheiten.

4) Support und Betreuung

(1) Die Keyuserin bzw. der Keyuser der Fraktion und die Vertreterin bzw. Vertreter sind für den First-Level-Support in der Fraktion zuständig und damit in der Fraktion Ansprechpartner/-innen für die Nutzerinnen und Nutzer in IT-Angelegenheiten. Falls die Keyuserin bzw. der Keyuser den benötigten Support fachlich nicht selbst leisten kann, werden die zentralen Ansprechpartner/-innen im IT-Referat kontaktiert („Second Level Support").

(2) Das IT-Referat leistet für die Fraktion den für den Betrieb benötigten „Second Level Support". Dieser umfasst neben der Sicherstellung der Funktionsfähigkeit der bereitgestellten IT-Infrastruktur sowie der Beseitigung von Störungen, sofern so vereinbart, auch die Pflege der Benutzerdaten im Active Directory bzw. im Benutzerverwaltungssystem „HaSI".

(3) Die Bürgerschaftskanzlei ist befugt, Dritte zur Erbringung von Service-Leistungen, Reparatur- oder Garantieleistungen zu beauftragen. Wenn diese Leistungen in den Räumen der Fraktionen erbracht werden, wird die Fraktion hierüber im Vorwege informiert.

(4) Die Servicezeiten des IT-Referates richten sich nach der geltenden Dienstvereinbarung der Bürgerschaftskanzlei zu einem flexiblen Dienstzeitmodell in der jeweils aktuellsten Fassung.

(5) Die Mitarbeiterinnen und Mitarbeiter des IT-Referates sind während der Servicezeiten über die IT-Hotline [redacted] telefonisch erreichbar. Für Anfragen, Mitteilungen oder Supportanfragen steht das Funktionspostfach [redacted] zur Verfügung.

5) Mitwirkungs- und Bereitstellungsleistungen der Fraktion

(1) Die zugesagten Leistungen erfordern Mitwirkungs- und Bereitstellungsleistungen der Fraktion. Die Fraktion stellt die vollständige und korrekte Übermittlung der Aufträge sowie der zur Bearbeitung von Aufträgen oder zur Störungsbeseitigung erforderlichen Daten sicher.

(2) Ergibt sich aus der Unterlassung von Mitwirkungspflichten oder aus der Nichtbereitstellung von Informationen oder Daten durch die Fraktion eine Auswirkung auf die Einhaltung dieser Anlage zu den Richtlinien, entlastet dies das IT-Referat von der Einhaltung der damit zusammenhängenden Leistung.

(3) Mit der Auslieferung der Komponenten geht die Verantwortung für den sachgerechten Umgang mit dem Gerät auf die Fraktion über. Für Schäden haften die Fraktionen entsprechend der gesetzlichen Regelungen.

6) Sicherheitsgrundlagen, Datenschutz

(1) Die Einrichtung und der Betrieb der bereitgestellten IT-Infrastruktur innerhalb des Datennetzes der Bürgerschaft orientieren sich an den in der FHH geltenden Grundsätzen und Richtlinien für Datenschutz und Datensicherheit (s. Anhänge). Diese dienen gleichermaßen dem Schutz und der Betriebssicherheit der IT-Infrastruktur der Fraktion, der Bürgerschaft sowie des gesamten Datennetzes der FHH.

(2) Die anzuwendenden Sicherheitseinstellungen ergeben sich aus den Vorgaben und Bestimmungen, die für den IT-Betrieb in der FHH gültig sind (s. Anhang A).

(3) Daneben dienen die Empfehlungen von Microsoft zur Verbesserung der Desktopsicherheit (Security Guidance Center) für Unternehmensclients sowie der BSI-Grundschutz-Standard (Bausteine: B 2.10 Mobiler Arbeitsplatz, B 3.201 Allgemeiner Client, B

3.203 Laptop, Betriebssysteme) als Orientierung bzw. Leitfaden für die Anwendung von Sicherheitsmaßnahmen (s. Anhang A17).

(4) Das IT-Referat sichert den vertraulichen Umgang mit Daten der Fraktionen zu. Die Mitarbeiterinnen und Mitarbeiter des IT-Referates verpflichten sich, insbesondere auch bei der Verwendung von Administrationskonten, eine Einsichtnahme in Dateiinhalte zu unterlassen.

(5) Damit das IT-Referat die vereinbarten Leistungen erbringen kann, ist es erforderlich, dass personenbezogene Daten der mit den Benutzerkonten verknüpften Personen der Fraktionen verarbeitet werden. Das IT-Referat pflegt und verwendet die Benutzerinformationen nach Vorgabe der Fraktion im Rahmen der Einrichtung und Pflege der Benutzerkonten im FHH-weiten System „HaSI".

Diese in HaSI vorgehaltenen personenbezogenen Daten sind entsprechend den gesetzlichen Vorschriften durch verschiedene Sicherheitssysteme angemessen gegen Missbrauch geschützt. Die Mitarbeiterinnen und Mitarbeiter von Dataport und der von Dataport beauftragten Firmen, die mit diesen personenbezogenen Daten umgehen, sind zur Verschwiegenheit verpflichtet.

7) IT-Ausstattung der Fraktion

Die der Fraktion auf Grundlage des § 2 a des Fraktionsgesetzes bereitgestellte IT-Infrastruktur umfasst nach derzeitigem Stand die nachfolgend beschriebenen Leistungen:

7.1) Ausstattung der Fraktion mit IT-Arbeitsplätzen (PC und Notebooks)

(1) Bemessungsgrundlage für die IT-Arbeitsplatzausstattungen der Fraktionen sind die den Fraktionen bereitgestellten Räume gemäß der „Anlage 1 zur Richtlinie zum Fraktionsgesetz". Die Anzahl der IT Arbeitsplatzausstattungen der Fraktionen wird daraus abgeleitet, so dass die IT Ausstattung mit der zur Verfügung gestellten Anzahl der Räume korreliert. Diese zugrunde gelegte Kalkulation wird im Anhang A weiter spezifiziert und fortgeschrieben.

(2) Der Fraktion werden PC-Arbeitsplätze zur Verfügung gestellt, die aus dem jeweils geltenden Rahmenvertrag der FHH beschafft werden. Das IT-Referat beschafft Geräte aus den jeweils verfügbaren Modelllinien, die für die jeweiligen Arbeitsplatzprofile und die eingesetzten Anwendungen geeignet sind und orientiert sich dabei an den üblichen Arbeitsplatzausstattungen in der FHH. Die Entscheidung über den Einsatz der jeweiligen Modelllinien wird zwischen Bürgerschaftskanzlei und den Fraktionsgeschäftsführungen getroffen. Die Nutzungsdauer für PC und Notebooks richtet sich grundsätzlich nach den Richtlinien der Finanzbehörde für die Kernverwaltung der FHH (derzeit: 5 Jahre) aus. Entsprechend dem 2017 festgestellten Bedarf wird die Nutzungsdauer für diese Ausstattung für beide Gerätetypen sowie verbundene Komponenten (Tastaturen, Bildschirme etc.) auf 4 Jahre festgelegt. Die PC-Ausstattung verbleibt im Eigentum der Bürgerschaft.

(3) Die von der Bürgerschaftskanzlei zur Verfügung gestellten IT-Arbeitsplätze verfügen über eine einheitliche Basisplattform, welche die folgenden Eigenschaften aufweist:

- PC bzw. Notebook, Bildschirm, Tastatur, Maus, Verbindungskabel
- Betriebssystem – die Version folgt den Standards der FHH-IT. Zeitlich erfolgt der Einsatz nach positivem Test der Verfahren und IT-Sicherheitsgrundlagen, die in der FHH genutzt werden
- Gesicherte Verbindung zum Datennetz der Bürgerschaft, der FHH und zum Internet
- Domänenanbindung der PC (Active Directory Domäne FHHNet)
- Virenschutz mit Anbindung an das zentrale Virenschutzmanagement (ePO)
- Anbindung an das zentrale Patch Management (WSUS)
- Anbindung an die „System Center Configuration Manager"-Infrastruktur (SCCM)
- einheitliche Sicherheitseinstellungen über Gruppenrichtlinien

(4) Die IT-Arbeitsplätze werden vom IT-Referat in Abstimmung mit den zuständigen Ansprechpartnern/-innen der Fraktion bereitgestellt, installiert und in Betrieb genommen. Zum Betrieb der bereitgestellten IT-Ausstattung zählt auch die Beseitigung von Störungen, bei Bedarf unter Einbeziehung der Lieferanten und Hersteller.

(5) Als mobile Clients werden Notebooks eingesetzt, die wechselweise innerhalb und außerhalb des Datennetzes der FHH betrieben werden können. Für jedes nach den Richtlinien zum Fraktionsgesetz zur Verfügung gestellte Notebook mit Telearbeitszugang wird eine UMTS-Vertragskarte aus den bestehenden FHH-Rahmenverträgen bereitgestellt.

7.2) Installierte Software

(1) Alle Clients werden einheitlich mit den nachfolgenden Komponenten ausgestattet:

- Basis-System: Das jeweils freigegebene Windows Betriebssystem und systemnahe Software wie Virenscanner und Softwareverteilung.
- Basis-Komponenten: Microsoft Office in der zum Betriebssystem und den verwendeten Anwendungen passenden Version, Internet-Explorer ab Vers. 11, verschiedene „Viewer" wie Acrobat Reader.

Eine Liste mit der aktuell standardmäßig bereitgestellten Software ist über den im Anhang A16 aufgeführten Link einsehbar. Die Lizenzen werden von der Bürgerschaftskanzlei bereitgestellt.

(2) Die Installation von Softwarekomponenten erfolgt grundsätzlich über eine automatisierte Softwareverteilung.

7.3) Bereitstellung von Servern und Diensten

(1) Zur Ablage von Daten für die Fraktion oder als Speicherort für persönliche Dateien wird der Fraktion ein Server (Fileserver) mit Laufwerken bereitgestellt. Diese Server-Laufwerke werden nach Systemstart und Anmeldung auf dem Client bereitgestellt und enthalten eine definierte Berechtigungsstruktur. Bereitgestellt werden:

- Laufwerk „F", "Gruppenlaufwerk", Datei-Ablagesystem für Arbeitsgruppen der Fraktion,
- Ein nicht sichtbares Laufwerk für Profildaten und Benutzereinstellungen,
- Laufwerk „Home" (derzeit „U"), Ablage für Outlook-Dateien und persönliche Daten,
- Laufwerk „Scanziele" (derzeit i.d.R. „Z"), Ablage für eingescannte Dokumente.
- Der Server wird als virtualisierter Server im Rechnerraum der Bürgerschaftskanzlei mit Einbindung in das Backup- und Überwachungsverfahren vorgehalten.

(2) Gruppendrucker und Arbeitsplatzdrucker werden über Druckdienste auf einem zentralen Druckserver der Bürgerschaftskanzlei angesteuert.

(3) Teile der für den IT-Betrieb benötigten Infrastruktur werden von Dataport bereitgestellt. Dazu zählen u.a. die Anmeldedienste (Active Directory), das Mailserver/Messagingsystem (MS Exchange), die Nutzung des Internet-Gateways mit Firewall mit zentralem Spam- und Virenschutz sowie die Nutzung von Kabel- und Netzwerkressourcen. Die Bürgerschaftskanzlei übernimmt die Kosten für den sog. Non-BASIS-Infrastrukturanschluss für die bereitgestellten Fraktionsarbeitsplätze.

(4) Sofern die Fraktion dies wünscht, wird die Mitnutzung der in der Bürgerschaftskanzlei eingesetzten Adressdatenbank „ZAM" mit eigenem Datenbestand (Mandanten) ermöglicht. Den Fraktionen der Bürgerschaft wird derzeit ein Kontingent von 10 Lizenzen für die gleichzeitige Nutzung zur Verfügung gestellt.

(5) Das IT-Referat betreibt ein System für die Bereitstellung von Daten in SharePoint. Dieses System wird von Dataport kostenpflichtig vorgehalten. Im Rahmen des- „Zuvex" – Verfahrens der FHH besteht die Zugriffsmöglichkeit von Arbeitsplätzen außerhalb des Netzes der FHH

(nach Authentifizierung). Für die Fraktionen wird eine Fraktions-Site zur Veröffentlichung von Informationen und zur Zusammenarbeit mit berechtigungsabhängigen Zugriffsmöglichkeiten für interne oder externe User bereitgestellt.

7.4) Netzwerk-Ausstattung

(1) Für den IT-Betrieb wird die bereitgestellte IT-Infrastruktur der Fraktionen eingebunden in das Datennetz der Bürgerschaft. Dieses Netzwerk ist wiederum angeschlossen an das von Dataport betriebene Datennetz der FHH mit gesicherten Übergängen zum Internet.

(2) Die Netzwerk-Anbindung der PC-Clients und Drucker in den Fraktionsräumen erfolgt durch das IT-Referat. Bereitgestellt werden folgende Komponenten:

- Für die auf Grundlage der Richtlinien zum Fraktionsgesetz genutzten Fraktionsräume außerhalb des Rathauses wird eine gebäudeübergreifende Netzwerkanbindung (zurzeit Glasfaserkabel) zum Datennetz der Bürgerschaft eingerichtet.
- Die Bürgerschaftskanzlei stellt in den Fraktionsräumen die für den Netzwerkbetrieb benötigten Komponenten bereit (Switches, Etagenverkabelung, Datendosen für PC und Telefone).

(3) Das Fraktionsnetz wird im Netzwerk der Bürgerschaft mit einem Netzwerk-Grundschutz eingerichtet (z.B. Verwendung von VLAN, Access-Lists, Einsatz einer Firewall).

7.5) Zusätzliche Ausstattungen

(1) Zusätzliche Hardwareausstattungen, Accounts oder Telearbeitsplätze, die benötigt werden und nicht Bestandteil der Ausstattung dieser Richtlinien zum Fraktionsgesetz sind (siehe: 2) Ziffer (3)), sind von den Fraktionen zu beschaffen und zu betreuen. Sofern diese zusätzliche IT-Ausstattung Bestandteil des Netzes der Bürgerschaft bzw. des Datennetzes der FHH sein soll, sind die Beschaffung, Einrichtung und der Betrieb mit dem IT-Referat abzustimmen.

(2) Die Administration wird vom IT-Referat mit übernommen, sofern es die dortigen Kapazitäten zulassen. Die der Bürgerschaftskanzlei entstehenden Sachkosten für Betrieb und Support (wie z.B. die Dataport Infrastruktur-Pauschale) trägt die Fraktion.

(3) Für die Produkte oder Dienstleistungen, die bei oder über Dataport beauftragt werden, werden Bestellung und Auftragsabwicklung im Einzelfall durch das IT-Referat der Bürgerschaftskanzlei unterstützt. Rechnungsempfängerin ist in diesem Fall die Fraktion.

(4) Optional kann nach Abstimmung zwischen Fraktionsgeschäftsführung und IT-Referat die Installation zusätzlicher Software-Komponenten aus den Warenkörben für FHH Basis-PC beauftragt werden. Sofern diese Software kein Bestandteil der IT-Arbeitsplatzausstattung im Sinne der Richtlinien zum Fraktionsgesetz ist, sind anfallende Kosten für Lizenzen, Paketierung und Installation von der Fraktion zu tragen. Informationen über die aktuellen vom ITAB[3] freigegebenen Software-Warenkörbe sind im FHH-Intranet abrufbar (siehe Anhang A16). Hierbei sind das Lizenzmanagement, die Softwareverteilung, die Handhabung von Updates und ggf. auch Fragen zu Netz- und Serverlasten einvernehmlich zu regeln.

(5) Softwareprodukte, die nicht vom ITAB (FHH IT Architecture Board) freigegeben sind, können innerhalb des Netzes der Bürgerschaft nicht verwendet werden. Ausnahme sind die in der Bürgerschaftskanzlei erstellten Softwarekomponenten (z.B. Datenbank Parlamentsdokumentation). Bei begründetem Bedarf kann nach Abstimmung zwischen Fraktionsgeschäftsführung und Bürgerschaftskanzlei eine alternative Lösung erarbeitet

[3]. Der Software-Standardwarenkorb (SWK) wird durch das ITAB festgelegt. Er bildet die Basis für die standardisierten IT-Arbeitsplätze. Der SWK enthält die für alle Behörden und Ämter der FHH übergreifend verfügbaren Softwareprodukte. Produkte, die von den Ämtern und Behörden benötigt werden und nicht im SWK enthalten sind, werden nach Freigabe in einem Kundenwarenkorb (KWK) pro Kunde zusammengefasst.

werden, wie beispielsweise die Installation auf PC außerhalb des Datennetzes der FHH oder die Verwendung anderer Produkte.

8) Betrieb und Administration der Arbeitsplatz-PC und Notebooks

8.1) Administration und Administrationsrechte

(1) Die Administration der der Fraktion zur Verfügung gestellten Geräte (PC, Notebooks, Server) und Verfahren liegt ausschließlich beim IT-Referat der Bürgerschaft. Die lokalen Kennungen der Administratorinnen und Administratoren sowie die BIOS-Passwörter verbleiben beim IT-Referat. Nur Mitarbeiterinnen und Mitarbeiter des IT-Referates der Bürgerschaftskanzlei haben OU-Administrationskennungen.

(2) Die Administration der Verfahren (u.a. Active Directory, Exchange-Dienste, SharePoint-Farm, Netzzugänge), die von Dataport bezogen werden, liegt bei den Administratoren der jeweiligen Fachbereiche bei Dataport.

8.2) Domäneneinbindung und Integration in das Active Directory (AD)

(1) Nach Durchlaufen der Installationsphase werden die PC oder Notebooks in das Active Directory (AD) der FHH eingebunden.

(2) Die Fraktions-PC und Server werden in einer eigenen Organisations-Einheit (OU) (z.B. „Fraktionen\SPD“) verwaltet.

8.3) Benutzerkonten (User Accounts) und Passwörter

(1) Der Zugang zu den PC-Systemen ist durch die Anmeldung mit Benutzername und Passwort geschützt. Auf jedem PC wird ein Bildschirmschoner mit aktiviertem Kennwortschutz eingerichtet. Die Latenzzeit bis zur Aktivierung der Bildschirmabschaltung beträgt 15 Minuten.

(2) Die Benutzerkonten sind persönliche Konten. Jede Benutzerin bzw. jeder Benutzer erhält ein eigenes persönliches Benutzerkonto (User Account) in der Domäne FHHNet. Für Praktikanten/Praktikantinnen und Referendare/Referendarinnen können generische Konten eingerichtet werden. Die PC-Benutzerkonten erhalten keine erweiterten Benutzer- oder Administrationsrechte.

(3) Die Vergabe von Kennwörtern richtet sich nach den in der FHH geltenden Passwort-richtlinien (Anhang A8). Passwörter sind vertraulich zu behandeln und nicht weiterzugeben.

(4) Für Gruppen und Funktionsträgerinnen/-träger in der Fraktion können zusätzlich in einem sinnvollen Umfang Benutzergruppen sowie Email-Funktions-Postfächer eingerichtet werden.

8.4) Einsatz von Gruppenrichtlinien

(1) Zum Einrichten und Verwalten der Benutzer- und Clientumgebungen werden Gruppen-richtlinien verwendet (vgl. Anhang A3). Die Benutzerrichtlinien legen die rollenspezifischen Sicherheitseinstellungen unabhängig von den verwendeten Endgeräten fest. Über die Clientrichtlinien werden wesentliche Sicherheitseinstellungen für die unterschiedlichen Endgeräte sowie Benutzereinstellungen eingestellt. Hierzu gehören u.a. folgende Bereiche:

- Basiseinstellungen und Konfiguration des Systems,
- Basiseinstellungen und Berechtigungsvergabe der Benutzerkonten,
- Systemdienste,
- Netzwerkkommunikation.

(2) Diese Gruppenrichtlinien orientieren sich an den in der FHH für BASIS-PC verwendeten Regeln, diese werden bei Bedarf durch das ITAB für BASIS-PC verbindlich fortgeschrieben.

(3) Die für die Fraktion angewendeten Gruppenrichtlinien können in begründeten Fällen auf Antrag der Fraktion und nach Abstimmung vom IT-Referat angepasst werden, sofern übergeordnete Sicherheitsinteressen nicht beeinträchtigt werden.

8.5) Datenhaltung, Benutzereinstellungen, Datensicherung des Clients

(1) Die Rechner sind so konfiguriert, dass die Nutzerdaten auf zentralen Systemen (File- und Profil-Server, SharePoint-Technologien etc.) gespeichert werden. Für die serverbasierte Ablage der Daten, sind auf dem Fraktionsserver Profil-, Home- und Gruppenlaufwerke eingerichtet.

(2) Die Benutzereinstellungen werden auf dem Fraktionsserver im Profilspeicher abgelegt. Innerhalb des Fraktionsnetzes ist „Roaming Profile" möglich, so dass die auf dem Server gespeicherten Profile an unterschiedlichen PC innerhalb der Fraktionen verwendet werden können.

(3) Der persönliche Systemordner „Eigene Dateien" wird über eine Ordner-Umleitung in das persönliche Home-Laufwerk umgeleitet.

(4) Bei den Notebooks mit Telearbeitszugang wird der Zugriff auf eine Festplattenpartition (Laufwerk „D") freigeschaltet, damit sich der Anwender/die Anwenderin über die Funktion „Offlinedateien" selbst ausgewählte Dateien und Ordner auch lokal verfügbar machen kann.

(5) Eine Datensicherung der auf dem Client abgelegten Daten erfolgt nicht, da der Zugang zu den lokalen Festplatten durch die Benutzer/-innen über Gruppenrichtlinien unterbunden ist. Die Daten der Anwender/-innen sind auf zentralen Systemen abgelegt (Fileserver, SharePoint-Technologien, etc.), die in festen Intervallen gesichert werden.

8.6) Internetzugang und –konfiguration

(1) Grundsätzlich erhalten alle Clients einen Internetzugang. Der Zugang zu Internet-Diensten wird über den zentralen Netzzugang von Dataport (Proxy-Server/Firewall) eingerichtet.

(2) Als Internet-Browser wird der Microsoft Internet Explorer zugelassen, weil nur dieser sich auf Basis der Gruppenrichtlinien zentral administrieren lässt. Der Internet Explorer wird so konfiguriert, dass die Sicherheitseinstellungen für die einzelnen Zonen zentral über Gruppenrichtlinien erfolgen (GPO). Daneben können auch andere Browser zur Internetrecherche bereitgestellt werden, sofern Begleitmaßnahmen oder technische Einstellungen die Sicherheit gewährleisten.

Dabei gelten zurzeit folgende Voreinstellungen:

- Lokales Intranet: niedrig,
- Internet: mittel,
- Vertrauenswürdige Sites: mittel,
- Eingeschränkte Sites: hoch.

Das IT-Referat kann diese Einstellungen zentral ändern, wenn dies aus Sicherheitsgründen von der Finanzbehörde veranlasst wird (z.B. bei einer globalen Virenattacke aus dem Internet). Die Fraktionen werden dann sofort informiert.

8.7) Externe Laufwerke und USB Schnittstellen

(1) Die Nutzung der USB-Schnittstellen an den Fraktions-PCs und Notebooks ist grundsätzlich möglich und freigeschaltet. Über Gruppenrichtlinien kann der Betrieb externer Geräte an USB-Schnittstellen unterbunden oder eingeschränkt werden, falls dies von der Fraktionsgeschäftsführung gewünscht wird. Die Fraktionen reduzieren das Risiko, Schadsoftware über USB-Schnittstellen in die Systeme einzuschleusen bspw. durch eine Verpflichtung der Mitarbeiterinnen und Mitarbeiter zur Sorgfalt und die Auswahl geprüfter externer Datenträger.

(2) Der Anschluss externer Speichermedien (Externe Laufwerke und USB-Speichersticks) wird unter Berücksichtigung der technischen Möglichkeiten so konfiguriert, dass:

- der Client-PC hierüber nicht gebootet werden kann,
- keine unkontrollierte Software ausgeführt oder eingespielt werden kann,
- Daten nicht unberechtigt kopiert oder anders verarbeitet werden können.

(3) Das Anschließen von Mobiltelefonen, Smartphones und anderen mobilen Endgeräten mit Datensynchronisation zu Mailboxen an Fraktions-PC ist aufgrund der in der FHH geltenden IT-Vereinbarungen ausschließlich mit Gerätetypen möglich, die vom ITAB freigegeben sind[4].

8.8) Fernadministration und Support-Aktionen

(1) Seit der Umstellung auf das Client-Betriebssystem Windows 7 wird die zentralisierte Administration (Fernzugriff und Fernadministration) unter Verwendung des „Microsoft System Configuration Manager" (*SCCM*) verstärkt eingesetzt. Für die folgenden Administrations-Aufgaben der Fraktions-Arbeitsplätze wird *SCCM* eingesetzt:

- automatisierte Softwareverteilung
- Fernadministration
- Inventarisierung und Reporting

Das IT-Referat stellt sicher, dass mit diesen Maßnahmen kein Zugriff auf Dateiinhalte erfolgt und keine Auswertung des Nutzerverhaltens vorgenommen wird.

(2) Seit der Einführung von Windows 7 nutzt das IT-Referat die Möglichkeit einer automatisierten Verteilung der eingesetzten Standard-Softwareprodukte. Hierbei werden vorkonfektionierte Softwarepakete über *SCCM* verteilt und verwaltet.

(3) Die Administratoren/-innen des IT-Referates haben die Möglichkeit, sich nach Zustimmung („Ja"-Klicken auf einem Ankündigungsfenster) auf den Bildschirm der Anwender/-innen aufzuschalten, um Anpassungen am System vorzunehmen oder bei der Bedienung zu unterstützen. Anwender/-innen und Administratoren/-innen sehen dann den gleichen Bildschirminhalt. Die Anwender/-innen können die Anfrage der Administratoren/-innen für eine Aufschaltung ablehnen und eine bereits zugestimmte und etablierte Aufschaltung jederzeit unterbrechen. Diese Maßnahme erleichtert die Administration (Reduzierung der „Turnschuh-Administration") und gibt auch den Anwendern/-innen die Möglichkeit, genau zu verfolgen, was auf dem PC passiert.

(4) Neben dem laufenden Messen der Füllgrade der zur Verfügung gestellten Speichersysteme können bei Bedarf und nach Absprache mit der Fraktionsgeschäftsführung Statistiken über die Datei- und Verzeichnisgrößen auf den Gruppenlaufwerken erstellt werden. Diese Maßnahme wird im Regelfall dann ausgelöst, wenn der Platzbedarf auf den Speichermedien stark angewachsen ist. Eine automatisiert erstellte Statistik ermöglicht die Analyse der Belegung der Speicher- und Datensicherungsmedien, so dass Problembereiche identifiziert werden können. Festgehalten werden u.a. die Speicherorte von großen Dateien, Dateitypen (Worddokumente, PDF, Grafiken, Mediadateien usw.), Datei-Eigentümer/-innen sowie Datum der Erstellung und des letzten Zugriffs. Anhand dieser Daten können Anwender/-innen nicht mehr benötigte Dateien löschen oder eine Auslagerung in Archiv-Verzeichnisse vornehmen.

Wegen der grundsätzlichen Sensibilität solcher Datenerhebungen werden diese Statistiken nur nach Ankündigung und nach Zustimmung durch die Fraktionsgeschäftsführung erhoben und ausgewertet. Die sich aus den Auswertungen ergebenden weiteren Maßnahmen werden mit der Fraktionsgeschäftsführung abgestimmt. Im Rahmen einer Störungsbeseitigung können

---

[4] Seit Juli 2012 stellt Dataport eine Möglichkeit bereit, iPhones/iPads über eine App (Excitor DME) mit dem FHH-Postfach zu verbinden, die mittlerweile auch für Android-SmartPhones zur Verfügung steht. Die Fraktionen haben die Möglichkeit, über das IT-Referat diesen Dienst bei Dataport auf eigene Kosten zu beantragen.

vom IT-Referat einzelne Auswertungen durchgeführt werden (z.B. Identifizierung von übergroßen Outlook-Archiven). Dateiinhalte werden zu keiner Zeit betrachtet oder ausgewertet. Die Statistiken werden vertraulich behandelt und nicht weitergegeben.

(5) Über die eingesetzte automatisierte technische Überwachung der PC werden technische Betriebsdaten erfasst, um Störungen oder das Überschreiten bestimmter Schwellwerte identifizieren zu können (z.B. Speicherfehler, Festplatten- oder Lüfterstörungen usw.). Außerdem können bestimmte Kenndaten des PC wie Prozessortype, Hauptspeicherbestückung, Seriennummer usw. automatisiert ausgelesen werden. Über die aktuellen Softwarestände und Lizenzinformationen kann ein Bericht generiert werden, ebenso über die Aktualität der Virenschutzprogramme oder der Sicherheitspatches.

8.9) Virenschutz

(1) Alle in der Fraktion betriebenen Rechner sind in den zentralen Virenschutz der Bürgerschaft integriert. Die Fraktions-PC werden dazu mit einem lokalen Virenscanner ausgestattet, der über das zentrale Virenschutzmanagement regelmäßig mit den aktuellen Signaturen und ggf. mit Updates und Fehlerkorrekturen versorgt wird.

(2) Der Virenschutz ist so eingerichtet, dass dieser von Anwendern/-innen nicht administriert oder deaktiviert werden kann. Ein vom Anwender/von der Anwenderin angestoßener Virenscan ist jederzeit möglich. Anwender/-innen können sich die Aktualität bzw. den Installationsstand der Virenschutzsoftware anzeigen lassen.

(3) Bei gefundener Schadsoftware wird die Virenschutzsoftware Maßnahmen ergreifen, die eine Aktivierung oder Verbreitung des Schadcodes verhindern, wie das Löschen oder das Verschieben der betroffenen Dateien in eine Quarantäne. Diese Aktivitäten werden im Virenschutzmanagement zentral erfasst und ausgewertet. Diese Informationen können ohne Bezug auf den Benutzer/die Benutzerin an die Sicherheitsteams der FHH (FB) bzw. bei Dataport weitergegeben werden.

(4) Bei begründetem Verdacht oder bei Feststellung des Vorhandenseins von Schadcode auf PC, der nicht automatisch von der Virenschutzsoftware entfernt werden kann, wird das IT-Referat den betroffenen Rechner unverzüglich vom Netzwerk trennen. Die betroffenen Anwender/-innen und die Fraktionsgeschäftsführung werden unverzüglich über den Vorfall und das weitere Vorgehen informiert.

8.10) Sicherheitspatches, Updates und Service Packs

(1) Die von Microsoft bereitgestellten Service Packs, Updates, Hotfixes und Patches werden über eine entsprechende Infrastruktur der Bürgerschaftskanzlei nach Maßgabe des Change- und Releasemanagement-Konzepts der FHH automatisch auf den Fraktions-PC installiert.

(2) Sicherheitspatches, die aufgrund ihrer Dringlichkeit (Stufe „kritisch“ oder „wichtig“) mit hoher Priorität auszurollen sind, können nach vorheriger Ankündigung, auch während des Betriebs, automatisch installiert werden, auch wenn der Betrieb (z.B. wegen eines Reboots) kurz unterbrochen werden muss.

(3) Patch- und Updatevorgänge werden vom IT-Referat dokumentiert. Diese Dokumentation kann den Sicherheitsbeauftragten der FHH in anonymisierten Auszügen übergeben werden.

(4) Sofern technisch möglich, werden Updates anderer Softwareprodukte (Adobe Flashplayer oder Acrobat, Java) automatisiert verteilt.

8.11) Anlegen, Löschen oder Migrieren von User-Accounts

(1) Das Anlegen, Ändern und Löschen von Benutzerkonten (User-Accounts) wird über das Verwaltungssystem „HaSI“ vorgenommen. Die Datenpflege über „HaSI“ wird vom IT-Referat vorgenommen. Sofern die Fraktion dies wünscht, kann die Datenpflege alternativ durch die

jeweilige Fraktion selbst vorgenommen werden. Die Fraktionen bleiben für die Richtigkeit der Adressbucheinträge selbst verantwortlich.

(2) Sofern die Datenpflege der Benutzerkonten vom IT-Referat vorgenommen wird, gelten folgende Verfahrensweisen:

- Neu anzulegende User-Accounts sind von der Fraktionsgeschäftsführung dem IT-Referat unter Angabe von Name, Vorname, Anrede, Titel, Funktion, Raumnummer, Telefon/Fax sowie Organisationseinbindung mitzuteilen. Durch Eintrag im Verwaltungssystem „HaSI" werden die neuen Benutzerkonten, Gruppenmitgliedschaften, Email-Accounts und Adressbucheinträge angelegt.
- Die Datenpflege vorhandener Accounts über „HaSI" wird vom IT-Referat nach entsprechender formloser Mitteilung der Änderungen durch die Fraktionsgeschäftsstelle vorgenommen.
- Ausscheidende Benutzerinnen oder Benutzer werden dem IT-Referat von der Fraktionsgeschäftsstelle mitgeteilt. Das IT-Referat löscht die Benutzerdaten, Adressbucheinträge und Postfächer über „HaSI". Ebenso werden die auf den Servern befindlichen Profil- und Home-Verzeichnisse gelöscht.

(3) Falls Daten aus den Postfächern oder Home-Laufwerken der ausscheidenden Mitarbeiterinnen oder Mitarbeiter der Fraktionen weiterhin benötigt werden, sind diese zuvor von den ausscheidenden Personen auf Gruppenlaufwerke zu verschieben.

(4) Alternativ können Benutzer-Accounts mit den dazugehörenden Postfächern, die nach dem Ausscheiden aus der Fraktion in einer Dienststelle im Behördennetz der FHH weiter verwendet werden sollen, in die nachfolgende Dienststelle verschoben werden. Diese Möglichkeit ist bei der Auftragsvergabe an das IT-Referat zu berücksichtigen. Die Übergabe der Accounts durch das IT-Referat erfolgt erst dann, wenn die Accounts von der Fraktionsgeschäftsführung freigegeben werden. Datenbestände in den Postfächern, die nicht mit migriert werden sollen, sind von der Fraktion zuvor zu verschieben oder zu löschen. Eventuell bestehende Weiterleitungen werden gelöscht.

8.12) Zugriffsrechte auf Datenbestände

(1) Die Zugriffsrechte auf die bereitgestellten Ressourcen werden prinzipiell über AD-Benutzergruppen geregelt. Die Gruppenstruktur folgt dem in der Domäne FHHNet verwendeten Kanon. In Abstimmung mit der Fraktionsgeschäftsführung oder mit den Keyusern oder Keyuserinnen wird eine Rollen- und Ressourcenstruktur festgelegt, die die in der Fraktion verwendeten Funktionen und die damit verbundenen Zugriffsmöglichkeiten auf die Dateisysteme der Fraktion adäquat abbildet.

(2) Das IT-Referat setzt im Auftrag der Keyuserin bzw. des Keyusers oder der Fraktionsgeschäftsführung die Berechtigungen auf die Laufwerke und Ordner der Filesysteme und trägt nach Vorgabe der Fraktion die Benutzer/-innen in die gewünschten Gruppen ein.

(3) Die Fraktion überwacht die Richtigkeit der Zugriffsberechtigungen selbst. Das IT-Referat stellt auf Anforderung eine Übersicht der verwendeten Benutzergruppen mit den eingetragenen Usern/Userinnen sowie ein Softwareprodukt zur Anzeige der in der Dokumentenablage gesetzten Zugriffsberechtigungen zur Verfügung.

8.13) Aussonderung von Client-PC

(1) Bei ausgesonderten Clients werden die entsprechenden Clientkonten und Zertifikate im Active Directory umgehend gelöscht.

(2) Beim Aussondern werden noch vorhandene Profil- und Benutzerdaten auf den lokalen Festplatten mit einem Programm zum sicheren Löschen so gelöscht, dass eine Wiederherstellung ausgeschlossen werden kann. Bei besonders sensiblen Daten kann die Fraktionsgeschäftsführung eine sichere Löschung der gesamten Festplatte verlangen. Die Clients können daraufhin vom IT-Referat bei Bedarf weiter eingesetzt werden.

9) Einrichtung und Betrieb von mobilen Clients

(1) Die Regelungen für Client-PC und Notebooks sind auch für die Einrichtung und den Betrieb von mobilen Clients (Telearbeitsplätze) anzuwenden. Ergänzend gelten folgende Regelungen:

(2) Die Benutzerin bzw. der Benutzer hat sicherzustellen, dass bei einer festen Netzwerkverbindung zum FHHNet der WLAN- oder UMTS-Modus stets abgeschaltet ist. Dies ist im Regelfall über einen am Gehäuse befindlichen Schalter möglich.

(3) Die mobilen Clients sind von der Benutzerin bzw. vom Benutzer nur mit FHHNet-Accounts verwendbar. Die mobilen Clients sind so konfiguriert, dass Internetverbindungen nur bei einer bestehenden Verbindung zum Netzwerk der FHH genutzt werden können.

(4) Zum Verbindungsaufbau mit dem Netzwerk der FHH werden die Notebooks mit Zusatzprodukten zum Aufbau eines VPN-Tunnels ausgestattet. Näheres hierzu ist im „Sicherheitskonzept für den Cisco VPN basierten mobilen Arbeitsplatz“ in der jeweils gültigen Fassung geregelt. Wegen der Einzelheiten wird auf die Anhänge A3, A4 und A5 verwiesen.

(5) Beim Einsatz von Wireless Local Area Network (WLAN) sind durch geeignete Maßnahmen ein sicherer Zugang zum FHHNET und ein sicherer Betrieb zu gewährleisten. Näheres hierzu ist im Sicherheitskonzept „WLAN-Infrastruktur“ in der jeweils gültigen Fassung (siehe Anhang A12) geregelt.

(6) Die Festplatten der mobilen Clients werden mit der standardmäßig vorhandenen Festplattenverschlüsselung ausgeliefert. Sofern auf den Geräten sensible Daten (z.B. personenbezogene Daten) verarbeitet werden, können die Festplatten der mobilen Clients auf Antrag der Fraktionsgeschäftsführung alternativ mit einer geeigneten Sicherheitssoftware zur Verschlüsselung ausgestattet werden.

10) Einrichtung und Betrieb von Servern

(1) Der der Fraktion zur Verfügung gestellte Server wird als virtueller Server, eingebunden in die virtuelle Serverinfrastruktur der Bürgerschaft, vorgehalten und in die Server- und Netzwerküberwachung der Bürgerschaft aufgenommen.

(2) Der zur Verfügung gestellte Speicherplatz für Gruppenlaufwerke, Homes- und Profillaufwerke wird aufgrund des verfügbaren Speicherplatzes auf den Massenspeichersystemen und der Kapazität der Datensicherung kontingentiert. Die Einzelheiten dazu werden im Anhang A weiter dokumentiert.

(3) Der Server und die auf den Server-Laufwerken befindlichen Daten sind eingebunden in das Datensicherungsverfahren (Backup) der Bürgerschaft:

- Vollsicherung sämtlicher servergespeicherter Daten einmal wöchentlich,
- eine tägliche Differenz-Sicherung (Sicherung aller Mutationen seit der letzten Vollsicherung).

Die Daten werden im sog. „Backup To Disc To Tape“-Verfahren gesichert. Die Datensicherungsbänder werden im Datenschrank aufbewahrt und nach Ablauf der Aufbewahrungsfrist überschrieben. Die Aufbewahrungsfristen der Datensicherungsbänder betragen zurzeit für Differenzsicherungen eine Woche und für Vollsicherungen ein Jahr.

(4) Die Fraktionsgeschäftsführungen oder Keyuser/-innen können dem IT-Referat unter Berücksichtigung der Aufbewahrungsfrist einen Auftrag zur Rücksicherung von Daten erteilen. Die zurückgesicherten Daten werden im Regelfall in den ursprünglichen Speicherorten mit den gespeicherten Zugriffsrechten zurückgesichert.

(5) Die Bestimmungen für Betrieb und Administration der Arbeitsplatz-PC und Notebooks gelten - sofern anwendbar - auch für den Betrieb der der Fraktion zur Verfügung gestellten

Server. Für den Betrieb von Servern, die bei Dataport betrieben werden, gelten die einschlägigen Service Level Agreements (SLA).

11) Einrichtung und Betrieb des Datennetzes

(1) Die Netzwerkkommunikation erfolgt auf Basis von TCP/IP über das Datennetz der Bürgerschaft zum Datennetz der FHH. Alle erforderlichen Netzwerkparameter werden über den DHCP-Server der Bürgerschaftskanzlei und durch Gruppenrichtlinien konfiguriert.

(2) Mit Ausnahme der für Telearbeit eingerichteten Notebooks ist eine Netzwerkkommunikation der Endgeräte ausschließlich über die vom IT-Referat bereitgestellten Netzwerkanschlüsse zu betreiben. Bei WLAN-fähigen Clients (Notebooks) ist vom Benutzer/von der Benutzerin sicherzustellen, dass bei einer Netzwerkverbindung zum FHHNet der WLAN- oder UMTS-Modus stets abgeschaltet ist.

(3) Server und Endgeräte der Fraktionen werden jeweils in einem eigenen virtuellen Netzwerksegment (VLAN) betrieben. Die Netzwerk-Switches werden seitens des IT-Referates so konfiguriert, dass nur dann eine Datenkommunikation zustande kommt, wenn das Endgerät für das VLAN zugelassen ist. Die Endgeräte können aus Sicherheitsgründen einem zugeteilten Port auf dem Netzwerk-Switch fest zugeordnet werden[5].

(4) Das IT-Referat setzt zur Trennung der Netzwerksegmente der Bürgerschaft und des Netzwerkes der FHH eine Firewall ein. Eine Speicherung der Protokolle des Datenverkehrs oder eine Auswertung von Inhalten erfolgt nicht. Protokolliert, kurzfristig gespeichert und bei Bedarf ausgewertet werden lediglich sicherheitsrelevante Inzidente (z.B. Viren- oder Schadcodeerkennung) sowie mögliche Zugriffsverletzungen (verworfene und abgelehnte Verbindungen).

12) Kontrollmechanismen, Überprüfungen

Neben den von der Bürgerschaftskanzlei einzurichtenden Kontrollmechanismen kann durch Informationssicherheitsbeauftragte der FHH (Finanzbehörde) als zuständige Überwachungsbehörde eine zusätzliche Überprüfung der Einhaltung der für die FHH geltenden Sicherheitsbestimmungen veranlasst werden. Innerhalb der FHH werden diese Überprüfungen entsprechend der Datenschutzrichtlinie (näheres siehe Anhang A11 DS-Richtlinie) in Verbindung mit den BSI-Grundschutzmaßnahmen M 2.25, M 2.330, M 4.146 und M 4.148 vorgenommen. Hierzu sind auf Anforderung vom IT-Referat geeignete Dokumentationen zur Verfügung zu stellen.

13) Schussbestimmungen, Inkrafttreten

(1) Diese Anlage wird bei Bedarf an aktuelle Gegebenheiten angepasst.

(2) Die Bestimmungen treten mit der Unterzeichnung der Richtlinie zum Fraktionsgesetz in Kraft und ersetzen die vorherige Version (Anlage 2 zu den Richtlinien zum Fraktionsgesetz in der Fassung vom 19.12.2012).

[5] Diese Maßnahme steht auch im Zusammenhang mit der von Dataport veranlassten Umstellung der konventionellen Telefontechnik auf netzwerkbasierte Telefonie (Projekt NGN).

Anhang A: Bemessungsrundlage für die IT-Ausstattung der Fraktionen

1) Arbeitsplatzausstattung

Die Bemessungsgrundlage für die IT Ausstattung der Fraktionen wurde auf Grundlage der Bemessung der Räume für die Fraktionen (siehe „Anlage 1 zur Richtlinie zum Fraktionsgesetz“) erstellt. Diese geht davon aus, dass die benötigte IT Ausstattung mit den zur Verfügung stehenden Räumlichkeiten (Anzahl der Räume und Raumgröße) korreliert.

Die Kalkulation ist in der Tabelle „2016-02-16 IT-Bedarf Fraktionen“ dokumentiert. Die darin enthaltene Tabelle „IT-Ausst. PC NB“ zeigt die Ableitung der IT-Ausstattung aus der Berechnung der Raumausstattung. Die Kalkulation berücksichtigt außerdem, dass den Fraktionen gemäß Ziff. II. 4 der Richtlinie zum FraktG. in der vorherigen Fassung zusätzliche Notebooks (je 1 Notebook pro Fraktion) zur Verfügung gestellt wurden.

Raumbezeichnung	Bemerkung	SPD	CDU	GRÜNE	Linke	FDP	AfD	Gesamt
Fraktionsvorsitz	Vorsitz	1	1	1	1	1	1	6
Fraktionsvorsitz	Stellvertretung	1	1	1	1	1	1	6
Geschäftsführung	Parlamentarische/r Geschäftsführer/in	1	1	1	1	1	1	6
Geschäftsführung	Fraktionsgeschäftsführer/-in	2	2	2	2	2	2	12
Pressestelle	Presse und Öffentlichkeitsarbeit	2	2	2	2	2	2	12
Öffentlichkeitsarbeit		1	1	1	1	1	1	6
Sekretariat des Fraktionsvorstandes	Sekretariat für 1 bis 2 Arbeitsplätze	2	2	2	2	2	2	12
Finanzbuchhaltung		1	1	1	1	1	1	6
Praktikantinnen, Referendarinnen		2	2	2	2	2	2	12
Arbeitsräume		15	10	7	5	5	4	46
Zuschlag RiLi FraktG. alte Vers.		1	1	1	1	1	1	6
Gesamt		29	24	21	19	19	18	130

Stand 05.12.2016

Die obige Tabelle ist ein Auszug aus der Datei „2016-02-16 IT-Bedarf Fraktionen“ mit Stand vom 05.12.2016. Diese berücksichtigt für die Kalkulation der IT-Arbeitsplätze die Anzahl der Mitglieder der Bürgerschaft pro Fraktion. Sie ist deshalb bei Veränderungen der Fraktionsstärke entsprechend fortzuschreiben.

Die Obergrenze für den Anteil von Notebooks bei der Arbeitsplatzausstattung wird unter Berücksichtigung der Nutzungsdauer, der Installationsaufwände und der Gerätekosten Ende 2017 mit 40% pro Fraktion festgelegt. Die tatsächliche Verteilung pro Fraktion sollte über den Nutzungszeitraum stabil bleiben, um Doppelbestellungen von Notebooks und PCs zu verhindern.

2) Datenvolumen auf den Fraktionsservern

Basierend auf der ermittelten Bemessungsgrundlage für die PC-Ausstattung wurde auch das auf den jeweiligen Fraktionsservern bereitgestellte Datenvolumen festgeschrieben. Die zur Verfügung stehende hochverfügbare Plattenspeicher- und Datensicherungskapazität erlaubt es, dass für die Fraktionen 15 GB/Arbeitsplatz bereitgestellt werden kann. Für dieses Datenvolumen werden sog. „Quotas“ (vom System erlaubtes max. Speichervolumen) auf den jeweiligen Fraktionsservern eingerichtet. Bei den zu verzeichnenden Zuwachsraten der vergangenen Jahre dürfte diese Speichermenge bis Ablauf des Abschreibungszeitraums der im Serverraum vorgehaltenen Infrastruktur ausreichen. Für die nächste Generation der Speicherkomponenten wird das benötigte Speichervolumen neu bewertet.

Die zugrunde gelegte Kalkulation ist in der Datei „2016-02-16 IT-Bedarf Fraktionen“ in dem darin enthaltenen Tabellenblatt „SpBedarf Frakt.“ dokumentiert.

Nr.	Auflistung der für die Bemessungsgrundlage relevanten Dokumente	Version/ Stand
1	**Excel-Tabelle „2016-02-16 IT-Bedarf Fraktionen“**	05.12.2016

Anhang B: Auflistung der in Zusammenhang mit den FHH Basis-Vorgaben für den Windows-Clientbetrieb stehenden Dokumente

Nr.		Version/ Stand
1	**Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern und sonstigen Endgeräten (PC-RL)** https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/PC-Richtlinie%2011.700%20(Änderung%20vom%2018.5.05).pdf	IT-Handbuch für die Verwaltung der Freien und Hansestadt Hamburg, 01.06.2005
2	**BASIS-Modelllinien-Technische Beschreibung** https://fhhportal.ondataport.de/websites/IT-Architekturboard_341/Allgemeine%20Dokumente/Hardware/HW_Neue_Modelle_01_2010.ppt	vom 12.01.2010
3	**Desktop-Management über Gruppenrichtlinienobjekte (GPO)** https://fhhportal.ondataport.de/websites/IT-Architekturboard_341/Protokolle/2007/070208%20Anlage%209%20Desktopmanagement%20über%20GPOs-V1_0.doc	Version 1.0 vom 08.02.2007
4	**Sicherheitskonzept für den Cisco VPN basierten mobilen Arbeitsplatz** https://fhhportal.ondataport.de/websites/IT-Architekturboard_341/Protokolle/2006/060828%20Anlage%20Sicherheitskonzept%20CMAP.doc	Dataport, Version 1.3 vom 22.08.2006
5	**Änderungen im Cisco VPN basierten Mobilen Arbeitsplatz (CMAP)** https://fhhportal.ondataport.de/websites/IT-Architekturboard_341/Protokolle/2006/061009%20Anlage%2019%20CMAP_060918.doc	09.10.2006
6	**Konformität von Programmen zum BASIS-PC** https://fhhportal.ondataport.de/websites/IT-Architekturboard_341/Protokolle/2006/061009%20Anlage%203%20Konformität%20von%20Programmen%20zum%20ESARI-PC%20V1_4.doc	Version 1.4 vom 05.10.2006
7	**Konzept zum Virenschutz- und Patchmanagement** https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/VPM-Konzept.pdf	IT-Handbuch für die Verwaltung der Freien und Hansestadt Hamburg, 01.06.2005
8	**Richtlinie zur Verwaltung von Passwörtern** https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/Passwort-Richtlinie%2011.650%20vom%2010.10.2007.pdf	IT-Handbuch für die Verwaltung der Freien und Hansestadt Hamburg, 10.10.2007

9	**Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung und Nutzung allgemeiner automatisierter Bürofunktionen und multimedialer Technik (Bürokommunikation) und zur Entwicklung von E-Government** https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/§93hmbpersvgvereinbarungen/Documents/94er-Buerokomm-pdf[1].pdf	05.05.2002
10	**Vereinbarung nach § 94 HmbPersVG über die Gestaltung der alternierenden Telearbeit in der hamburgischen Verwaltung** https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/§93hmbpersvgvereinbarungen/Documents/Telearbeit%20(2005).pdf	16.12.2005
11	**Richtlinie zur Datensicherheit im IuK-Bereich (DS-Richtlinie) vom 6. September 2006 (MittVw Seite 90)** https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/Datensicherheit%20im%20IuK-Bereich%2011.100.pdf	IT-Handbuch für die Verwaltung der Freien und Hansestadt Hamburg, 01.10.2006
12	**Sicherheitskonzept: WLAN-Infrastruktur** https://fhhportal.ondataport.de/websites/IT-Architekturboard_341/IT-Architekturboardsitzungen%202010/Dokumentbibliothek/20100223/20100216%20WLAN-Sicherheitskonzept_WLAN-Infrastruktur_v2.0.doc	16.02.2010
13	**Telekommunikationsrichtlinie (TK-RL)** https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/Telekommunikationsrichtlinie%2012.000.pdf	IT-Handbuch für die Verwaltung der Freien und Hansestadt Hamburg, 22. April 2016
14	**Vorgaben zum Windows-Client-Betrieb in der Freien und Hansestadt Hamburg** https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/20120925%20WCV%20V1.21%20final.pdf	Finanzbehörde V 1.2.1 vom 25.09.2012
16	**Freigegebene Softwareprodukte Basis Warenkörbe ITAB** https://fhhportal.ondataport.de/websites/IT-Architekturboard_341/Sitzung17/Freigegebene%20Dokumente/171114%20TOP%203%20Anlage%203%20Status_SWK.pptx	
17	**Katalog der BSI-Grundschutzmaßnahmen für Windows-Clients** https://www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html	
18	Rahmen-Sicherheitskonzept der Freien und Hansestadt Hamburg https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/20150623%20Rahmen-SiKo-FHH_V1.00.pdf	Finanzbehörde V 1.0 vom 23.06.2015
19	Informationssicherheitsleitlinie für die Freie und Hansestadt Hamburg http://fhhportal.stadt.hamburg.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/Informationssicherheitsleitlinie-FHH%20Vers_1%20vom%2020130402.pdf	FHH V 1.0 vom 02.04.2013

Glossar

Active Directory (AD): Verzeichnisdienst von Microsoft Windows Server. (Ab der Version Windows Server 2008 wird die Kernkomponente als Active Directory Domain Services (ADOS) bezeichnet) Das Active Directory ermöglicht es, ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung zu gliedern. Dazu verwaltet es verschiedene Objekte in einem Netzwerk wie beispielsweise Benutzer/-innen. Gruppen, Computer, Dienste, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften. Mit Hilfe von Active Directory kann ein Administrator/eine Administratorin die Informationen der Objekte hierarchisch organisieren, bereitstellen und überwachen.

BSI-Grundschutz: Die IT-Grundschutz-Kataloge (vor 2005: IT-Grundschutzhandbuch) sind eine Sammlung von Dokumenten des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), die der Erkennung und Bekämpfung sicherheitsrelevanter Schwachstellen in IT-Umgebungen dienen. Die Sammlung umfasst mit Einleitung und Katalogen über 4000 Seiten und dient als Grundlage zur Zertifizierung des IT-Grundschutzes eines Unternehmens.

ePO: McAfee ePolicy Orchestrator. Werkzeug zur Administration und Überwachung der Sicherheitsprodukte der Fa. McAfee (Security and Compliance Management).

DHCP: ermöglicht die automatische Einbindung eines Computers in ein bestehendes Netzwerk ohne dessen manuelle Konfiguration. Beim Start des Rechners (Client) am Netz wird die IP-Adresse, die Netzmaske, das Gateway, DNS-Server von einem DHCP-Server bezogen.

First-Level-Support: Der First-Level-Support ist die erste Anlaufstelle für alle eingehenden Unterstützungsfragen. Die Mitarbeiterin oder der Mitarbeiter (Keyuserin bzw. Keyuser) ist für deren vollständige Erfassung inklusive aller erforderlichen Zusatzinformationen zuständig und bearbeitet sie nach vorhandenem Kenntnisstand weitestgehend selbstständig. Ziel ist die Selektion, das schnelle Lösen oder die qualifizierte Weitergabe des Problemfalls an die nächste Instanz. Unterstützung erhält der First-Level-Support durch den Second-Level-Support.

HaSI: Das HamburgService-Informationssystem liefert als „Government Directory" aktuelle Daten über Organisation, Dienstleistungen, Zuständigkeiten und Ansprechpartner/-innen der Hamburger Behörden, Die Daten in HaSI werden über eine Software dezentral von den Behörden und Ämtern gepflegt und zentral gespeichert. Über HaSI werden neben den Personendaten für den HamburgService, den Behördenfinder im Internet und die Behördenrufnummer 115 u.a. auch die Benutzerkonten im Active Directory der FHH gepflegt.

ITAB: IT Achitecture Board. Die Aufgaben des FHH Gremiums sind u.a. die Vorbereitung und Initiierung der Umsetzung von IT-Strategievorhaben, die Initiierung der Fortschreibung der IT-Architekturrichtlinie, die Umsetzung von Entscheidungen in Fragen der IT-Interoperabilität und IT-Sicherheitsstandards sowie die Festlegung und Fortschreibung der Standardwarenkörbe (SWK) und bilden damit die Basis für die standardisierten IT-Arbeitsplätze der FHH. Die Geschäftsführung des ITAB liegt bei der FB, dauerhafte, stimmberechtigte Mitglieder des ITAB sind 7 IT-Leiter sowie Vertreterinnen und Vertreter der FB, Dataport und des LGV.

Keyuser: Der Begriff Key-User wurde erstmals im Zuge der Einführung betriebswirtschaftlicher Software (z.B. ERP-Systeme) genutzt. Die Keyuserin bzw. der Keyuser selbst ist eine Mitarbeiterin bzw. ein Mitarbeiter des Unternehmens und vertritt die fachlichen Interessen des Fachbereiches in Projektteams und fungiert als Ansprechpartnerin oder Ansprechpartner für die Kolleginnen und Kollegen der eigenen Abteilung gegenüber Anbietern/-innen, Projektleitern/-innen und IT-Teams.

OU: (siehe auch Active Directory) Die Vielzahl der Objekte in einem großen Unternehmensnetzwerk (Domäne) werden in Containern (Organisationseinheiten, OU, Organizational Unit) abgelegt. Einige Container sind vordefiniert, weitere Organisationseinheiten können mit Unterorganisationseinheiten erstellt werden. Als objektbasiertes System unterstützt das Active Directory die Vererbung von Eigenschaften eines Objektcontainers an untergeordnete Objekte oder Objektcontainer. Dadurch erlaubt es Active Directory, Netzwerke logisch und hierarchisch aufzubauen. Die Bürgerschaftskanzlei und Fraktionen stellen mit eigenen OU's adressierbare Container im AD der FHH dar.

NGN: Next Generation Network ermöglicht das klassische Telefonieren über Computer Netzwerk-technik. Dazu nutzen Telefon und Computer streckenweise dieselbe Netzwerk-Infrastruktur. An einem zentralen Punkt wird ein Übergang in das öffentliche Telefonnetz bereitgestellt. Mit NGN können weitere Funktionen für Anwender bereitgestellt werden (z.B. Videokonferenz, Sofortnachricht auf dem PC usw.).

SAN: Als Storage-Area-Network (SAN) bzw. Speichernetzwerk bezeichnet man die Anbindung von Festplattensubsystemen an Server-Systeme über Hochgeschwindigkeitsnetzwerke. Storage Area Networks sind für serielle, kontinuierliche Hochgeschwindigkeitsübertragungen großer Datenmengen konzipiert worden. Sie basieren auf hochverfügbaren und hochperformanten Installationen auf Basis des Fibre-Channel-Standards.

SCCM: System Center Configuration Manager ist ein Software-Produkt von Microsoft zur zentralisierten Verwaltung von Hard- und Software innerhalb eines Unternehmens. Folgende Aufgaben können von SCCM automatisiert für eine sehr große Anzahl von Clients durchgeführt werden: Inventarisierung, Softwareverteilung, Fernwartung, Lizenzüberwachung und Reporting. Auf dem zu verwaltenden Endgerät (SCCM Client) läuft im Hintergrund die SCCM Client Software mit den aufgabenbezogenen Agenten.

Second-Level-Support: Der Second-Level-Support unterstützt den First-Level-Support, sowohl durch Weiterbildung am Arbeitsplatz (engl. training-on-the-job) als auch durch Übernahme komplexerer Anfragen durch Spezialisten/Spezialistinnen. Übersteigt die Komplexität einer Anfrage das Know-how oder die technischen Möglichkeiten des Second-Level-Supports, so wird diese an den Third-Level-Support (z.T. Externe) weitergeleitet („eskaliert"). Der Third-Level-Support setzt sich aus Spezialisten/Spezialistinnen einzelner Fachbereiche oder des Herstellers zusammen und stellt so die höchste Eskalationsstufe innerhalb einer Supportorganisation dar.

TCP/IP: Transmission Control Protocol/Internet Protocol (TCP/IP) ist eine Familie von Netzwerkprotokollen und wird wegen ihrer großen Bedeutung für das Internet auch als Internetprotokollfamilie bezeichnet. Innerhalb eines TCP/IP-Netzwerkes (weltweit oder auch Firmennetzwerke) geschieht die Identifizierung der am Netzwerk teilnehmenden Rechner über sog. IP-Adressen.

UMTS: Das Universal Mobile Telecommunications System (UMTS) ist ein Mobilfunkstandard der dritten Generation (3G), mit dem deutlich höhere Datenübertragungsraten (bis zu 21 Mbit/s mit HSPA+) als mit dem Mobilfunkstandard der zweiten Generation (2G), dem GSM-Standard (bis zu 220 kbit/s bei EDGE; sonst max. 55 kbit/s bei GPRS), möglich sind.

VLAN: Ein Virtual Local Area Network (VLAN) ist ein logisches Teilnetz innerhalb eines physischen Netzwerks. Es kann sich über einen oder mehrere Switches hinweg ausdehnen. Ein VLAN trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switches die Datenpakete (Frames) eines VLANs nicht in ein anderes VLAN weiterleiten, und zwar auch dann nicht, wenn die Teilnetze an gemeinsame Switches angeschlossen sind.

VPN-Tunnel: Ein Virtual Private Network (deutsch „virtuelles privates Netz", kurz „VPN, dient dazu, Teilnehmer eines Netzes an ein anderes Netz anzubinden, ohne dass sich die Netzwerke in unmittelbarer räumlicher Nähe zueinander befinden müssen. Der externe VPN-Teilnehmer kann sich über eine Internetverbindung mit der Anschlussstelle (VPN-Gateway) des anderen Netzes verbinden, so als wäre sein Netzwerkanschluss direkt am anderen Netz angeschlossen. Diese Verbindung (VPN-Tunnel) wird durch eine zusätzliche Verschlüsselung ergänzt, so dass eine abhör- und manipulationssichere Kommunikation zwischen den VPN-Partnern ermöglicht wird.

WLAN: Wireless Local Area Network (oder auch „drahtloses lokales Netzwerk", Wireless LAN, W-LAN, Wi-Fi). bezeichnet ein lokales Funknetz, basierend auf Standards der IEEE-802.11-Familie, zur Verbindung von mobilen Endgeräten mit einem fest stationierten Netzwerkübergang. Dazu stehen diverse Protokolle für eine gesicherte und verschlüsselte Verbindung zur Verfügung (z.B. WPA2).

WSUS: Windows Server Update Services (WSUS) ist die Softwarekomponente des Microsoft Windows Server 2003 und Microsoft Windows Server 2008, die für die Überwachung und (automatisierte) Verteilung von Patches und Aktualisierungen von Microsoft Produkten eingesetzt wird.

Zuvex: Zuvex ist eine auf dem Microsoft Unified Access Gateway basierende Lösung im Datennetz der FHH und stellt ein Weiterleitungsmodul dar, das wie eine Kombination aus VPN-Tunnel und Firewall arbeitet. Dadurch kann der Nutzer sicher von seinem Browser aus dem Internet heraus auf ausgewählte Anwendungen aus dem FHHNet zugreifen. Zusätzlich wird, um sowohl die Sicherheit für die Nutzer als auch für das FHHNet zu gewährleisten, bei der Anmeldung auf dem genutzten PC eine Endgerätekontrolle durchgeführt. Bei dieser wird auf sicherheitsrelevante Aspekte, wie eine aktive Firewall und einen aktuellen Virenschutz geprüft. Die Zugriffsrechte auf die Verfahren werden also in Abhängigkeit vom Sicherheitsstandard des zugreifenden Geräts gewährt.

Quellen: Diverse Internetportale, insbesondere Wikipedia (Texte z.T. gekürzt oder leicht abgewandelt); FHH Portal.