Sicherheitshinweise zu den Online-Wahlen der Goethe-Universität im Sommersemester 2021

1. Allgemeines

Die universitären Gremienwahlen zum Senat und zu den Fachbereichsräten werden im Sommersemester 2021 als Online-Wahl durchgeführt.
Es bestand die Möglichkeit, bis zum 19.05.2021 im Wahlamt Briefwahl zu beantragen. Mit dem Versand oder Aushändigung der Briefwahlunterlagen sind die Wahlberechtigten von der Online-Wahl ausgeschlossen.

Wahlberechtigte, die keinen Antrag auf Briefwahl gestellt haben, können **im Zeitraum vom 14.06.2021, 13:00 Uhr bis 25.06.2021, 15:00 Uhr** ihre Stimme online abgeben.

Die Onlinewahl ist browserbasiert und betriebssystemunabhängig weltweit von den EDV-Endgeräten der Wahlberechtigten ohne Installation einer Spezialsoftware möglich sowie einfach und intuitiv zu navigieren, somit kann die Stimmabgabe innerhalb der Wahlfrist orts- und zeitunabhängig erfolgen. Als technische Plattform wird das Wahlsystem POLYAS der POLYAS GmbH mit der auf die universitätsspezifischen Bedürfnisse angepassten Nutzerführung des Wahlsystems eingesetzt. An POLYAS wurde 2016 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland erstmals das Zertifikat für eine Onlinewahl-Software erteilt. Es basiert auf den Common Criteria für Onlinewahlen und dem Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, die sich aus den allgemeinen Wahlgrundsätzen ableiten. Dementsprechend sind Online-Wahlen in der Konfiguration Polyas CORE 2.2.3 nach Maßgabe der BSI Anforderungen sicher und erfüllen die Ansprüche an das demokratische Wahlrecht.

2. Sicherheitshinweise

Allgemeine Sicherheitshinweise

Die Abstimmung durch die Wahlberechtigten erfolgt bei den als Onlinewahl durchgeführten Wahlen auf einem individuell genutzten EDV-Endgerät mit Internetanschluss (z.B. Arbeitsplatzrechner, Tablet, PC, Notebook, Smartphone), über welches die abgegebenen Stimmen verschlüsselt an das Wahlsystem übertragen werden.
Die Beachtung der hier empfohlenen Sicherheitsmaßnahmen soll sicherstellen, dass geeignete Vorkehrungen getroffen sind, um ein Mindestmaß an Sicherheit zu gewährleisten und Angriffe durch „Computerviren, Würmer, Trojaner“ (Schadprogramme) und ähnliche dienstebehindernde Attacken auf dem Computerarbeitsplatz und auf den Wahlservern zu vermeiden sowie die persönliche Einhaltung des Wahlgeheimnisses zu gewährleisten.

Falls Sie weitere Informationen zur Absicherung von Rechnersystemen benötigen, wenden Sie sich an die für Ihr System zuständigen Administratoren oder informieren Sie sich mittels folgender Ressourcen:

Webseite IT-Sicherheit

https://www.rz.uni-frankfurt.de/hrz/it-sicherheit

Webseite des SMT

https://www.uni-frankfurt.de/smt

IT-Sicherheitsrichtlinie der GU

https://www.uni-frankfurt.de/75452541/IT_Sicherheitsrichtlinie.pdf

BSI für Bürger

https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html

Nutzbarkeit des Wahlsystems trotz technischer oder persönlicher Einschränkungen
Die Wahlanwendung ist grundsätzlich für alle berechtigten Nutzerinnen und Nutzer unabhängig von deren körperlichen und / oder technischen Möglichkeiten weitgehend uneingeschränkt ohne besondere Erschwernis und in der allgemein üblichen Weise zugänglich und kann grundsätzlich ohne fremde Hilfe genutzt werden (barrierearm). Dies schließt sowohl die Nutzung durch Personen mit und ohne gesundheitliche Beeinträchtigungen, als auch die Nutzung mit technischen Einschränkungen (z.B. Textbrowser oder PDA) grundsätzlich ein. Das Vorlesen der dargestellten Informationsangebote über spezielle Computerprogramme (Screenreader) oder die Ausgabe in Braille-Schrift für Blinde und sehbehinderte Personen ist mit entsprechenden Hilfsmitteln möglich.

3. Wahlsystem

Bei der Onlinewahl der Goethe-Universität kommt das Wahlsystem POLYAS der POLYAS GmbH (www.polyas.de) zum Einsatz. Das Wahlsystem besteht aus drei technischen Modulen: Online-Wahlsystem von POLYAS läuft auf räumlich und systemisch getrennten Teilsystemen und besteht aus drei technischen Modulen:

1. Das Modul Wählerverzeichnis enthält ein anonymes Verzeichnis, in dem lediglich die Wahlnummern und keine personenbezogenen Daten enthalten sind.
2. Das davon getrennte Modul Wahlfreigabe (Validator) erteilt die Wahlmöglichkeit.
3. Das gleichfalls unabhängige Modul Wahlurne wird für die Aufbewahrung und Zählung der Stimmen eingesetzt.

Als Übertragungskanal wird bei der Onlinewahl das Internet genutzt. Das Online-Wahlsystem gewährleistet, dass die Kommunikation zwischen den Modulen mittels des als hinreichend sicher geltenden Protokolls „https“ mit SSL-Zertifikaten ausschließlich verschlüsselt und somit gesichert erfolgt. Daten, welche auf die persönliche Identität von Wahlberechtigten schließen lassen könnten, werden ausdrücklich NICHT im Wahlsystem gespeichert. Um den Datenschutz bei der Online-Wahl zu wahren, wird von vornherein ausgeschlossen, personenbezogene Daten an die Fa. POLYAS zu übermitteln. Das Wählerverzeichnis wird anonymisiert, bevor es an die Fa. POLYAS weitergeleitet wird. Die Sicherheit der für den Betrieb eingesetzten Server – die streng getrennt arbeiten – sowie die dort eingesetzten Verfahren werden durch die technischen Betreiber nach allgemein anerkannten Sicherheitsstandards gewährleistet.

4. Sicherheitstechnische Anforderungen an das EDV-Endgerät, das zur Durchführung der Wahl genutzt wird

Zur Durchführung des Wahlvorgangs ist ein handelsübliches EDV-Endgerät mit funktionierendem Internetanschluss erforderlich, wie er in den Einrichtungen der Goethe-Universität und auch in vielen Privathaushalten üblich ist. Es wird empfohlen, ausschließlich EDV-Endgeräte in vertrauenswürdigen Umgebungen zu nutzen, bei denen die grundsätzliche Einhaltung der empfohlenen Sicherheitsmaßnahmen im Allgemeinen sichergestellt wird. Diese Sicherheit wird z. B. in den Computerpools oder den Arbeitsplatzrechnern der Goethe-Universität gewährleistet. Von der Nutzung von EDV-Endgeräten in nicht vertrauenswürdigen Umgebungen wird aus Sicherheitsgründen abgeraten. Wahlberechtigte sind grundsätzlich selbst dafür verantwortlich, dass die Beachtung der hier empfohlenen Sicherheitsmaßnahmen am genutzten EDV-Endgerät gegeben ist.

5. Zugang zur Wahl, Benutzerautorisierung über das HRZ-Account

Die Anmeldung zur Online-Wahl erfolgt durch die Eingabe des HRZ-Accounts [1], mit dem sich die Wahlberechtigten für die Wahl auch authentifizieren. . Der Wahlserver kann nur aus dem Universitätsnetz unter „https://wahlen.uni-frankfurt.de“ erreicht werden.

Wahlberechtigte Personen befinden sich innerhalb des Universitätsnetzes:

Wahlberechtigte Personen, die sich bereits im Universitätsnetz befinden (z.B. über ihren gewohnten VPN-Client oder vor Ort), können den Link:‘https://wahlen.uni-frankfurt.de‘ direkt nutzen. Nach der Anmeldung mit ihrem HRZ-Account in die Eingabemaske werden die Wahlberechtigten auf das Online-Wahlsystem von POLYAS geleitet und können direkt ihre Stimme abgeben. Die Identität der Wählerin oder des Wählers ist zu jeder Zeit geschützt.

Wahlberechtigte Personen befinden sich außerhalb des Universitätsnetzes:

Für die Wahlberechtigten außerhalb des Universitätsnetzes wird eine separate VPN-Einwahl (https://vpn-wahlen.uni-frankfurt.de) zur Verfügung gestellt, über welche sie sich nach Authentifizierung mittels HRZ-Account in das Universitätsnetz einwählen können. Nach dieser Authentifizierung befinden sich die Wahlberechtigten im Universitätsnetz und ihnen wird der Anmeldebereich der URL ‘https://wahlen.uni-frankfurt.de‘ angezeigt. Nach der erneuten Anmeldung mittels HRZ-Account in die Eingabemaske werden die Wahlberechtigten auf das Online-Wahlsystem von POLYAS geleitet und können ihre Stimme abgeben.

Den HRZ-Account erhalten die Studierenden mit i der Einschreibung und die Beschäftigten mit Beginn ihres Arbeits- oder Dienstverhältnisses bei der Goethe-Universität. Für den Fall, dass Wahlberechtigten der HRZ-Account nicht mehr bekannt sein sollte, können sie sich an den Service-Bereich des Hochschulrechenzentrums telefonisch unter: 069/798 77710 oder per Mail: goethecard@rz.uni-frankfurt.de wenden.

6. Wahlvorgang

Nach der erfolgreichen Anmeldung im Wahlsystem Polyas werden den Wahlberechtigten die elektronischen Stimmzettel derjenigen Gremien angezeigt, für die sie wahlberechtigt sind. Im nächsten Schritt können die Wahlberechtigten einen oder mehrere Wahlvorschläge auf den angezeigten Stimmzetteln markieren und werden anschließend zur Bestätigung ihrer Wahl aufgefordert. Nach der Bestätigung werden die abgegebenen Stimmen auf den markierten Stimmzetteln bis zur Auszählung in der elektronischen Wahlurne anonym gespeichert. Ein erneutes Einloggen mit dem HRZ- Account ist nach Bestätigung der Stimmabgabe nicht mehr möglich.

7. Automatische Zeitüberwachung/Abmelden vom Wahlsystem

Verlassen Sie das Wahlsystem bitte ordnungsgemäß über die Schaltfläche "Wahl abbrechen / ausloggen" (oben), wenn Sie den Wahlvorgang ab- oder unterbrechen wollen. Sollten Sie einmal versäumt haben, die Wahlanwendung zu beenden oder längere Zeit Ihren Rechner unbeaufsichtigt lassen, bricht die im Wahlsystem eingebaute Zeitsperre aus Sicherheitsgründen den Wahlvorgang ab, sobald ca. 15 Minuten lang keine Eingabe erfolgt ist. Die von Ihnen durchgeführten Aktionen werden dabei ausdrücklich nicht gespeichert! In beiden vorgenannten Fällen müssen Sie sich daher erneut mit Ihren Zugangsdaten am Wahlsystem anmelden und die von Ihnen durchgeführten Aktionen wiederholen.

[1] Der HRZ- Account besteht aus dem Login (auch Username oder (Be-)Nutzerkennung genannt) und dem Passwort.

8. Geheimhaltung der Zugangsdaten
Bitte achten Sie unbedingt darauf, dass Sie Ihre Zugangsdaten (Nutzername und Passwort) immer unter Verschluss halten und unberechtigte Dritte keinen Zugriff auf diese Daten bekommen.

9. Nutzung des EDV-Endgerätes ohne administrative Rechte
Wir empfehlen Ihnen dringend, das Internet nur mit einem Benutzerkonto ohne Administrationsrechte zu nutzen. Schadprogramme sind zur dauerhaften Installation auf fremden Rechnern meist darauf angewiesen, dass angemeldete Benutzerinnen oder Benutzer über Administrationsrechte verfügen. Wie Sie ein solches Benutzungskonto ohne diese Rechte einrichten, können Sie der Dokumentation Ihres Betriebssystems entnehmen.

10. Einsatz von Computerprogrammen aus vertrauenswürdigen Quellen
Installieren und starten Sie keine Programme, die Sie von Unbekannten oder ungefragt von Bekannten per E-Mail oder aus anderen unsicheren Quellen erhalten haben. Vorsicht: Auch Bildschirmschoner sind Programme. Sofern auch nur geringe Zweifel an der Vertrauenswürdigkeit von Programmen bestehen, sollten Sie auf eine Installation auf Ihrem Rechner verzichten.

11. Software zum Anzeigen von Internetseiten (Browser)
Zur Anzeige der im Internet (World Wide Web) angebotenen Informationen (Webseiten) werden spezielle Computerprogramme (Browser) zum Betrachten eingesetzt. Achten Sie darauf, dass Sie die eingesetzte Browser-Software aus vertrauenswürdigen Quellen bezogen haben, sodass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt. Bitte setzen Sie nur vom Hersteller freigegebene Versionen der Internet-Browser ein. Beim Bekanntwerden von Sicherheitsproblemen veröffentlichen die Softwarehersteller in der Regel zeitnah fehlerbereinigte Versionen (Updates). Informieren Sie sich daher regelmäßig über neue Sicherheitsupdates für das Betriebssystem und den Browser Ihres EDV-Endgerätes.

Unterstützte Browser

Die Stimmabgabe erfolgt ausschließlich mit folgenden Browsern:

- Chrome
- Safari
- Firefox
- Opera
- Edge

Wichtig ist jedoch, dass Sie die jeweils aktuellste Version Ihres Internetbrowsers auf Ihrem Gerät installiert haben.

Sicherer Umgang mit dem Browser bezüglich der Wahlen

Um eine möglichst hohe Sicherheit und Vertraulichkeit beim Umgang mit den Wahlsystemen zu gewährleisten, wird beim Durchführen der Wahl folgende Vorgehensweise empfohlen:

1. Schließen Sie alle offenen Webbrowserfenster auf Ihrem EDV-Endgerät.
2. Starten Sie einen Browser, der unter Punkt vier aufgelistet ist, mit dem Sie die Wahl durchführen möchten und geben die Webadresse zur Wahlseite ein. Alternativ klicken Sie auf den Link zur Wahl, so dass dieser sich im Standardbrowser öffnet.
3. Führen Sie die Wahl in diesem Browserfenster durch.
4. Schließen Sie erneut alle Webbrowserfenster.

Indem bei der Durchführung der Wahl exklusiv nur diese Webseite geöffnet ist und der Browser danach wieder komplett geschlossen wird, sollen potentielle Restrisiken bezüglich des Webbrowsers reduziert werden.

12. Schutz vor dem Ausspähen von Benutzerdaten

Durch sogenannte "Trojanische Pferde" (als Trojanisches Pferd, auch kurz Trojaner genannt, bezeichnet man ein Programm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen der nutzenden Person eine andere, meist unerwünschte Funktion erfüllt) können vertrauliche Daten ausgespäht und während einer Internetsitzung von Ihnen unbemerkt an Dritte übertragen werden („Phising“). Dadurch besteht das potenzielle Risiko, dass Ihre Zugangsdaten bei der Eingabe über die Tastatur abgefangen und an Unberechtigte gesendet werden, die dann z.B. an Ihrer Stelle wählen könnten. Einen begrenzten Schutz gegen derartige Trojaner können auch sogenannte Anti-Spy-Programme bieten, die als lizenzierte, kostenpflichtige Produkte oder als Freeware (unentgeltlich nutzbare Computerprogramme) zur Verfügung stehen. Als Spyware wird üblicherweise Software bezeichnet, die persönliche Daten ohne Wissen oder Zustimmung von Nutzerinnen oder Nutzern eines Computers an Dritte sendet.
Darüber hinaus sollten Sie auch Software zur Fernwartung (z.B. teamviewer) deaktivieren, um sicherzustellen, dass keine unbefugte Person den Wahlvorgang mitverfolgen kann und damit die Geheimheit der Wahl verletzt.

13. Überwachung des Datenverkehrs vom und zum Internet

Zusätzlichen Schutz vor "Trojanischen Pferden" können auch sogenannte Personal Firewalls bieten, die als lizenzierte, kostenpflichtige Produkte oder als Freeware zur Verfügung stehen. Dies sind Programme, die, richtig eingestellt, den gesamten Datenverkehr von und zum Internet überwachen. Sie können dadurch erkennen und verhindern, wenn ein anderes Programm als der von Ihnen benutzte Browser versucht, Datenpakete über das Internet zu versenden.
Bezugsquellen für Virenschutz-Software, Personal Firewalls und Anti-Spy-Programme finden Sie in Computer-Zeitschriften sowie an vielen Stellen im Internet.

14. Hilfestellungen bei Problemen und Fragen

Für die Durchführung des Wahlvorgangs finden Sie eine Anleitung auf der Internetseite des Wahlamtes unter:https://www.uni-frankfurt.de/97451003/Senats__und_FbRwahlen_2021.

Wenn Sie eine sicherheitsrelevante Unregelmäßigkeit bemerken oder einen Verdacht auf Manipulation haben, wenden Sie sich bitte sofort an das Wahlamt der Goethe-Universität.

Kontaktinformationen

Sofern sich in Bezug auf Ihren persönlichen Computerarbeitsplatz technische Probleme oder Fragen ergeben sollten, wenden Sie sich bitte unmittelbar an die Zuständigen für das Rechnernetz, an das der von Ihnen genutzte Computerarbeitsplatz angeschlossen ist.

Kontakt:

Wahlamt der Goethe-Universität
Campus Westend | PA-Gebäude
Theodor-W. Adorno-Platz 1
60323 Frankfurt am Main
3. OG | Raum 3. P.53
wahlamt@uni-frankfurt.de

Ansprechpartner*in:

Ayten Agdas
agdas@em.uni-frankfurt.de
Tel. +49 (0)69 798-17174

Dr. Suat Suna
s.suna@em.uni-frankfurt.de
Tel. +49 (0)69 798-17411