Georg-August-Universität Göttingen
Sicherheitshinweise zu den digitalen Wahlen
im Wintersemester 2023/2024

I. Allgemeines

Die Wahlen an der Georg-August-Universität Göttingen zu den Kollegialorganen, zu den Studentischen Organen (inkl. Urabstimmungen) sowie zur Promovierendenvertretung werden im Wintersemester 2023/2024 als internetbasierte digitale Wahlen (im Folgenden: Onlinewahlen) mit Briefwahlmöglichkeit durchgeführt. Die Onlinewahl ist browserbasiert und betriebssystemunabhängig weltweit von EDV-Endgeräten ohne Installation einer Spezialsoftware möglich sowie einfach und intuitiv zu navigieren. 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 und 2021 erneuert. 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 2.5.3 und 2.5.4 nach Maßgabe der BSI-Anforderungen sicher und erfüllen die Ansprüche an das demokratische Wahlrecht.

II. Allgemeine Sicherheitshinweise

Die Abstimmung durch die Wahlberechtigten erfolgt bei den als Onlinewahl durchgeführten Wahlen auf einem individuell genutzten EDV-Endgerät mit Internetzugang (z.B. Arbeitsplatzrechner, Tablet, PC, Notebook, Smartphone), über welches die Stimmen verschlüsselt an das Wahlsystem übertragen werden.

Die Beachtung der hier empfohlenen Sicherheitsmaßnahmen soll sicherstellen, dass geeignete Vorkehrungen getroffen sind, um ein möglichst hohes Sicherheitsniveau zu gewährleisten und Angriffe durch „Computerviren, Würmer, Trojaner“ (im Folgenden: Schadprogramme) und ähnliche dienstebehindernde Attacken auf dem EDV-Endgerät und auf den Wahlservern zu verhindern sowie die persönliche Einhaltung des Wahlgeheimnisses zu gewährleisten.

Bitte beachten Sie auch die für alle Mitglieder und Angehörigen der Georg-August-Universität Göttingen (einschließlich UMG) geltende Informationssicherheitsrichtlinie (https://www.uni-goettingen.de/de/informationssicherheitssrichtlinie/52744.html).

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

Zur Durchführung des Wahlvorgangs ist ein übliches EDV-Endgerät mit funktionierendem Internetzugang erforderlich, wie es auch in den Einrichtungen der Georg-August-Universität und in vielen Privathaushalten üblich ist. Es wird angeraten, 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 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.

IV. Geheimhaltung der Zugangsdaten

Bitte achten Sie unbedingt darauf, dass Sie Ihre Zugangsdaten (Matrikelnummer und Passwort) sorgsam behandeln und unberechtigten Dritte keinen Zugriff auf diese Daten ermöglichen. Ihr Passwort halten Sie bitte unter Verschluss.

V. 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.

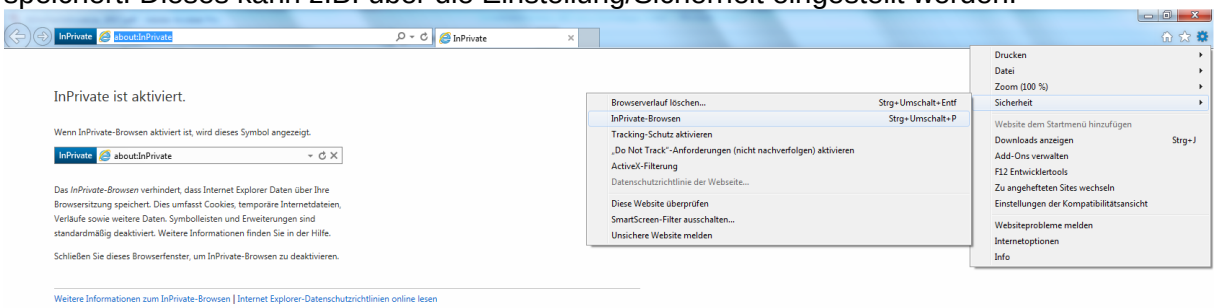
VI. Einstellungen der Browser

Die Internet-Browser verschiedener Herstellerfirmen unterscheiden sich zwar in ihrer Handhabung und Konfiguration; einige Hinweise haben aber allgemeingültigen Charakter. Folgende Punkte sollten Sie beachten:

Sie sollten während der Nutzung des Wahlsystems darauf verzichten, in einem zweiten Browser-Fenster andere Internetseiten mit nicht vertrauenswürdigen Inhalten anzuzeigen. Die Internetseiten des Wahlsystems benötigen für ihre Funktionsfähigkeit nicht das von Microsoft entwickelte Softwarekomponenten-Modell ActiveX für die Anzeige aktiver Inhalte. Da mit Hilfe von ActiveX auch Zugriffe auf die Daten und Komponenten Ihres Computers möglich sind, wird empfohlen, ActiveX im Browser generell zu deaktivieren. Die Aktivierung der objektbasierten Programmiersprache Javascript, die häufig zur Unterstützung von benutzungsbezogenen Funktionen in internetbasierten Anwendungen eingesetzt wird, ist erforderlich. Stellen Sie Ihren Browser so ein, dass verschlüsselte Seiten und sogenannte Cookies zum Speichern Ihrer persönlichen Einstellungen auf Webseiten nicht gespeichert werden.

Deaktivieren Sie die Funktion, welche Benutzernamen und Kennwörter für die automatische Eingabe bei späteren Aufrufen speichert. Sie finden diese Einstellungen häufig unter „Autovervollständigen“, oder sie heißen z.B. Kennwort- oder Password-Manager. Sorgen Sie dafür, dass der sogenannte Cache (Speicherbereich, in dem zuvor angezeigte Seiten gespeichert werden) des Browsers nach jeder Sitzung gelöscht wird. Durch diese Maßnahme können Sie verhindern, dass die auf dem von Ihnen benutzten EDV-Endgerät aufgerufenen Seiten nachträglich angesehen werden können. Sie können dafür zum Beispiel die Tastenkombination „Strg + Shift + Entf“ verwenden. Je nach Browser haben Sie dann die Möglichkeit, den Cache zu löschen.

Sie können die Browser aber auch im „Privaten Modus“ verwenden. Dabei nutzen Sie das Internet, ohne dass der Browser Daten über Ihre Webseitenbesuche auf Ihrem Rechner speichert. Dieses kann z.B. über die Einstellung/Sicherheit eingestellt werden.



VII. Sichere verschlüsselte Übertragung

Grundlage einer sicheren Internetverbindung ist die Verwendung eines sogenannten sicheren Protokolls für die verschlüsselte Übertragung der Daten (SSL oder Secure Sockets Layer bezeichnet ein Netzwerkprotokoll zur sicheren Übertragung von Daten u.a. von

Internetseiten). Das Bestehen einer solchen sicheren SSL-Verbindung wird Ihnen bei Verwendung z.B. von Firefox und Mozilla durch ein geschlossenes Schloss-Symbol angezeigt. Bitte achten Sie darauf, dass nach der Anmeldung am Wahlsystem während der Verbindungsdauer dieses Symbol als „geschlossen“ dargestellt wird. Durch Doppelklick auf das jeweilige Symbol werden Ihnen weitere Informationen zum Sicherheitszertifikat angezeigt. Die Darstellung ist abhängig von der von Ihnen eingesetzten Browserversion. Die Serverzertifikate der Wahlserver können Sie anhand der dazu gehörenden sogenannten elektronischen Fingerabdrücke (fingerprints) prüfen. Hierzu überprüfen Sie bitte – wie zuvor beschrieben – die Internet- Adresse (URL), mit der Sie verbunden sind.

Als URL muss "https://election.polyas.com“ angezeigt werden. Die Internetadresse muss während einer Sitzung mit "https://" angezeigt werden und nicht mit "http://". Das 's' in https signalisiert eine sichere Verbindung.

Das Zertifikat des Servers (*polyas.com) hat folgende Fingerprints:

- SHA-1
  A5:2E:2D:05:C3:58:DF:9A:14:3B:58:BF:BC:D4:44:10:3B:D0:B9:8A

- SHA-256
  8A:72:DB:F3:42:F2:0D:C8:10:5D:9C:98:4F:91:A7:E4:CA:88:D3:57:D1:E3:AB:00:F6:1D:5F:95:43:C8:AE:C8

Sofern Sie diese Daten angezeigt bekommen, besteht eine sichere und verschlüsselte Verbindung zum Wahlsystem. Sollten Sie andere Daten angezeigt bekommen, beenden Sie die Verbindung sofort und informieren Sie bitte umgehend die Wahlleitung (die Kontaktdaten finden Sie insbesondere am Ende dieser Sicherheitshinweise, auf der Seite www.uni-goettingen.de/Wahlen, in der Wahlbenachrichtigung, in der Wahlausschreibung, in der Wahlbekanntmachung oder im Wahlsystem).

VIII. Nutzung des EDV-Endgeräts ohne administrative Rechte

Wir empfehlen dringend, das Internet (bzw. interne Netzwerke und externe Datenträger) nur mit einem Benutzer*innenkonto ohne Administrationsrechte zu nutzen; die universitären Accounts verfügen üblicherweise nicht über administrative Berechtigungen. Schadprogramme sind zur dauerhaften Installation auf fremden Rechnern meist darauf angewiesen, dass angemeldete Benutzer*innen über Administrationsrechte verfügen. Wie Sie ein solches Benutzungskonto ohne diese Rechte einrichten, können Sie der Dokumentation Ihres Betriebssystems entnehmen.

IX. 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 (Firefox, Mozilla, Opera, Safari, Edge etc.) 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-Endgeräts, z.B. für Microsoft-Produkte mit Hilfe der Windows-Update-Funktion unter http://www.update.microsoft.com.

X. Einzelheiten zum Schutz vor Schadprogrammen

1. Schutz vor Computerviren

Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Einmal gestartet, kann es von der*dem Benutzer*in nicht kontrollierbare Veränderungen am Status der Hardware (z.B. Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion). Computerviren können durch von der erstellenden Person gewünschte oder nicht gewünschte Funktionen die Computersicherheit beeinträchtigen. Installieren Sie daher einen Virenscanner auf Ihrem Computerarbeitsplatz und lassen Sie diesen regelmäßig alle Dateien auf Viren überprüfen (scannen). Achten Sie darauf, dass Sie ständig (täglich) die neuesten Aktualisierungen (Updates) einspielen, die alle führenden Herstellerfirmen von Virenscannern anbieten.

2. 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 Nutzer*innen 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.

3. Überwachung des Datenverkehrs vom und zum Internet

Zusätzlichen Schutz vor Schadprogrammen, insbesondere „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 vom 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.

4. Bezugsquellen für Schutzprogramme

Mitglieder der Universität finden hier Informationen:

- https://docs.gwdg.de/doku.php?id=de:services:it_security:virus_protection:start#bitdefender-service_der_gwdg

Weitere Informationen und nützliche Tipps zum Thema Sicherheit im Internet erhalten Sie auch hier:

- http://www.bsi-fuer-buerger.de

XI. Nutzbarkeit des Wahlsystems trotz technischer oder persönlicher Einschränkungen

Die Wahlanwendung ist grundsätzlich für alle berechtigten Nutzer*innen 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.

XII. Wahlsystem

Bei der Onlinewahl kommt das Wahlsystem POLYAS der POLYAS GmbH (www.polyas.de) zum Einsatz. Das Wahlsystem besteht aus drei technischen Modulen. Das Modul Wählerverzeichnis enthält ein anonymes Verzeichnis, in dem lediglich die Wahlnummern und keine personenbezogenen Daten enthalten sind. Das davon getrennte Modul Wahlfreigabe (Validator) erteilt die Wahlmöglichkeit und das gleichfalls unabhängige Modul Wahlurne wird für die Aufbewahrung und Zählung der Stimmen eingesetzt. Als Übertragungskanal wird bei der Onlinewahl das Internet genutzt. Die Kommunikation zwischen den Modulen erfolgt mittels des – als hinreichend sicher geltenden – Protokolls „https“ ausschließlich verschlüsselt. Daten, welche auf die persönliche Identität von Wahlberechtigten schließen lassen könnten, werden NICHT im Wahlsystem gespeichert. 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.

XIII. Autorisierung über einen universitären Benutzer*innen-Account

Die Wahlberechtigten melden sich mittels Eingabe der Matrikelnummer und des Passworts (des Benutzer*innen-Account der Universität) über das Wahlportal der Universität unter https://onlinewahl.uni-goettingen.de/onlinewahl an. Nach der Anmeldung prüft das System, ob die*der Benutzer*in wahlberechtigt ist, und erzeugt daraufhin eine temporäre URL (SecureLink) zum Wahlsystem. Eine weitere Anmeldung am Wahlsystem ist nicht notwendig; die Wahlberechtigten können direkt mit der Stimmabgabe beginnen. Die Identität der*des Wählerin*Wählers ist geschützt.

XIV. Abmelden vom Wahlsystem / Automatische Zeitüberwachung /

Verlassen Sie das Wahlsystem bitte ordnungsgemäß über die Schaltfläche "Wahl abbrechen/ausloggen" (oben), wenn Sie den Wahlvorgang ab- oder unterbrechen wollen. Wenn Sie sich eingeloggt haben und für 15 Minuten inaktiv waren, werden Sie automatisch ausgeloggt. Dies dient der Sicherheit Ihrer Stimmabgabe; natürlich wird Ihre bisherige Stimmauswahl in diesem Fall nicht (zwischen)gespeichert wird. Sie können sich innerhalb des Wahlzeitraums erneut anmelden und digital wählen.

XV. Briefwahl

Bis zum 02. Januar 2024; 15:00 Uhr (Ausschlussfrist) konnte bei der Wahlleitung ein Antrag auf Briefwahl eingereicht werden. Mit dem Versand oder der Aushändigung der Briefwahlunterlagen sind die Wahlberechtigten von der Onlinewahl ausgeschlossen.

XVI. Hilfestellungen bei Problemen und Fragen

Für die Durchführung des Wahlvorgangs finden Sie über die Internetseite: www.uni.goettingen.de/wahlen Anleitungen oder Hilfestellungen. Für vertiefende Fragestellungen steht Ihnen darüber hinaus eine ausführliche Wahlanleitung online im Wahlsystem zur Verfügung.

Wenn Sie eine sicherheitsrelevante Unregelmäßigkeit, z.B. eine Manipulation, bemerken, wenden Sie sich bitte sofort an die Wahlleitung der Universität.

XVII. Kontaktinformationen

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

Kontakt:

Wahlleitung der Georg-August-Universität Göttingen
Abteilung Wissenschaftsrecht und Trägerstiftung
Bereich 81
Von-Siebold-Straße 2
37075 Göttingen
https://www.uni-goettingen.de/wahlen

Ansprechpartner:

Ralf Buhre
ralf.buhre@zvw.uni-goettingen.de
Tel. +49 551 39-28093

Georg-August University Göttingen
Security advice for the digital elections
in the winter semester 2023/2024

I. General

The elections at the Georg-August-Universität Göttingen for the collegial bodies, the student bodies (incl. ballots) and the doctoral students' representation will be held in the winter semester 2023/2024 as internet-based digital elections (hereinafter: online elections) with the option of postal voting. The online election is browser-based and operating system-independent, possible worldwide from IT end devices without the installation of special software, and easy and intuitive to navigate. The POLYAS voting system from POLYAS GmbH is used as the technical platform, with the user guidance of the voting system adapted to the university-specific needs. POLYAS was awarded the certificate for online voting software by the Federal Office for Information Security (BSI) in Germany for the first time in 2016 and renewed in 2021. It is based on the Common Criteria for online elections and the basic set of security requirements for online election products, which are derived from the general election principles. Accordingly, online elections in the Polyas CORE 2.5.3 and 2.5.4 configuration are secure in accordance with the BSI requirements and meet the requirements for democratic voting.

II. General security instructions

In the case of elections conducted as online elections, voting by those entitled to vote takes place on an individually used EDP terminal device with Internet access (e.g. workplace computer, tablet, PC, notebook, smartphone), via which the votes are transmitted to the voting system in encrypted form.

Observance of the security measures recommended here is intended to ensure that suitable precautions are taken to guarantee the highest possible level of security and to prevent attacks by "computer viruses, worms, Trojans" (hereinafter: malware) and similar service-impeding attacks on the EDP terminal device and on the election servers, as well as to guarantee personal compliance with the secrecy of the ballot.

Please also observe the Information Security Guideline (https://www.uni-goettingen.de/de/informationssicherheitssrichtlinie/52744.html) applicable to all members and staff of the Georg-August-Universität Göttingen (including UMG).

III. Security requirements for the EDP terminal device used to conduct the election

In order to carry out the voting process, a standard EDP terminal device with functioning Internet access is required, as is also customary in the institutions of the Georg-August University and in many private households. It is advisable to use only IT terminals in trustworthy environments where basic compliance with the recommended security measures is generally ensured. This security is guaranteed, for example, in the computer pools or the workstation computers of the university. The use of computer terminals in untrusted environments is discouraged for security reasons. As a matter of principle, persons entitled to vote are themselves responsible for ensuring that the security measures recommended here are observed on the IT terminal used.

IV. Confidentiality of access data

Please make absolutely sure that you handle your access data (personal or matriculation number and password) with care and do not allow unauthorised third parties access to this data. Please keep your password under lock and key.

V. Use of computer programmes from trustworthy sources

Do not install or start any programmes that you have received from unknown persons or unsolicited from acquaintances by e-mail or from other unsafe sources. Caution: Screen

savers are also programmes. If there is even a slight doubt about the trustworthiness of programmes, you should refrain from installing them on your computer.

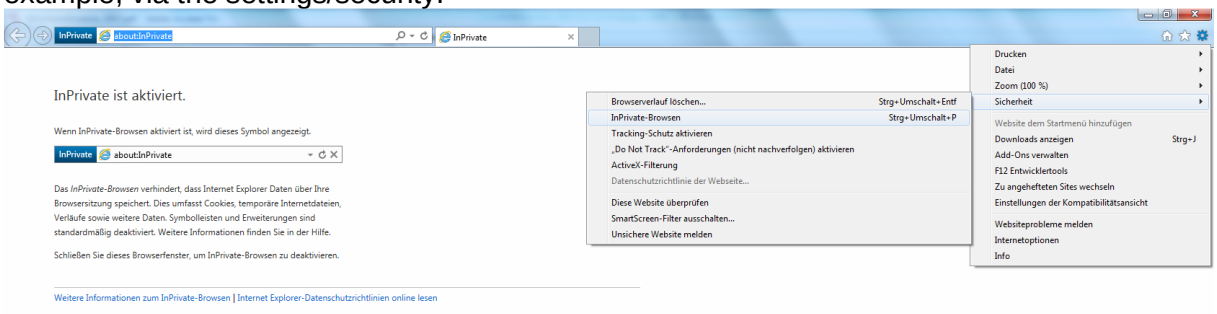
VI. Browser Settings

The Internet browsers of various manufacturers differ in their handling and configuration; however, some tips are generally valid. You should observe the following points:

You should refrain from displaying other Internet pages with untrustworthy content in a second browser window while using the voting system. The Internet pages of the voting system do not require the ActiveX software component model developed by Microsoft for the display of active content in order to function. Since ActiveX can also be used to access the data and components of your computer, it is recommended to generally deactivate ActiveX in the browser. Activation of the object-based programming language Javascript, which is often used to support user-related functions in Internet-based applications, is required. Set your browser so that encrypted pages and so-called cookies for saving your personal settings on websites are not saved.

Deactivate the function that saves user names and passwords for automatic entry on subsequent calls. You will often find these settings under "Autocomplete", or they are called password or password manager, for example. Make sure that the so-called cache (memory area in which previously viewed pages are stored) of the browser is deleted after each session. By taking this measure, you can prevent the pages called up on the EDP terminal you are using from being viewed subsequently. You can use the key combination "Ctrl + Shift + Del" for example. Depending on the browser, you then have the option of deleting the cache.

You can also use the browsers in "private mode". In this mode, you use the internet without the browser saving data about your website visits on your computer. This can be set, for example, via the settings/security.



VII Secure encrypted transmission

The basis of a secure Internet connection is the use of a so-called secure protocol for the encrypted transmission of data (SSL or Secure Sockets Layer refers to a network protocol for the secure transmission of data, e.g. from Internet pages). The existence of such a secure SSL connection is indicated to you by a closed lock symbol when using e.g. Firefox and Mozilla. Please note that after logging on to the voting system, this symbol is displayed as "closed" during the connection period. Double-click on the respective symbol to display further information on the security certificate. The display depends on the browser version you are using. You can check the server certificates of the election servers by means of the so-called electronic fingerprints belonging to them. To do this, please check - as described above - the internet address (URL) to which you are connected.

The URL must be "https://election.polyas.com". During a session, the internet address must be displayed with "https://" and not with "http://". The 's' in https signals a secure connection.

The certificate of the server (*polyas.com) has the following fingerprints:

- SHA-1
  A5:2E:2D:05:C3:58:DF:9A:14:3B:58:BF:BC:D4:44:10:3B:D0:B9:8A

- SHA-256
  8A:72:DB:F3:42:F2:0D:C8:10:5D:9C:98:4F:91:A7:E4:CA:88:D3:57:D1:E3:AB:00:F6:1D:5F:95:43:C8:AE:C8

If these data are displayed, there is a secure and encrypted connection to the voting system. If you are shown other data, terminate the connection immediately and inform the election administration (the contact details can be found in particular at the end of these security instructions, on the page www.uni-goettingen.de/Wahlen, in the election notification, in the election announcement, in the election notice or in the election system).

VIII. Use of the computer terminal without administrative rights

We strongly recommend that you only use the internet (or internal networks and external data media) with a user account without administrative rights; university accounts do not usually have administrative rights. Malware is usually dependent on logged-in users having administrative rights in order to be permanently installed on other people's computers. How to set up such a user account without these rights can be found in the documentation of your operating system.

IX. Software for displaying Internet pages (browser)

Special computer programmes (browsers) are used to display the information (web pages) offered on the Internet (World Wide Web). Make sure that you have obtained the browser software used from trustworthy sources to ensure that it is unmodified original software. Please only use versions of Internet browsers (Firefox, Mozilla, Opera, Safari, Edge, etc.) that have been approved by the manufacturer. When security problems become known, the software manufacturers usually publish bug-fixed versions (updates) in a timely manner. Therefore, inform yourself regularly about new security updates for the operating system and browser of your computer, e.g. for Microsoft products using the Windows update function at http://www.update.microsoft.com.

X. Details on protection against malware

1. Protection against computer viruses

A computer virus is a self-replicating computer program that infiltrates other computer programs and thus reproduces itself. The classification as a virus refers to the spreading and infection function. Once started, it can make changes to the status of the hardware (e.g. network connections), the operating system or the software that cannot be controlled by the user (malicious function). Computer viruses can compromise computer security through functions desired or not desired by the person creating them. Therefore, install a virus scanner on your computer workstation and have it regularly check (scan) all files for viruses. Make sure that you constantly (daily) install the latest updates (updates) offered by all leading virus scanner manufacturers.

2. protection against the spying out of user data

So-called "Trojan horses" (a Trojan horse, also called a Trojan for short, is a programme that is disguised as a useful application, but in the background fulfils another, usually unwanted function without the knowledge of the person using it) can spy out confidential data and transfer it to third parties unnoticed by you during an Internet session ("phising"). This poses the potential risk of your access data being intercepted when you enter it via the keyboard and sent to unauthorised persons who could then, for example, vote in your place. So-called anti-spyware programmes, which are available as licensed, chargeable products or as freeware (computer programmes that can be used free of charge), can also offer limited protection against such Trojans. Spyware is usually software that sends personal data to third parties without the knowledge or consent of the user of a computer.

In addition, you should also deactivate software for remote maintenance (e.g. teamviewer) to ensure that no unauthorised person can follow the voting process and thus violate the secrecy of the election.

3. monitor data traffic to and from the internet.

Additional protection against malware, especially "Trojan horses", can also be provided by so-called personal firewalls, which are available as licensed, chargeable products or as freeware. These are programmes that, when set up correctly, monitor all data traffic to and from the internet. They can thus detect and prevent when a programme other than the browser you are using tries to send data packets over the Internet.

Sources of anti-virus software, personal firewalls and anti-spyware can be found in computer magazines and many places on the Internet. 4.

4. sources of supply for protection programmes

Members of the university can find information here:

- https://docs.gwdg.de/doku.php?id=de:services:it_security:virus_protection:start#bitdefender-service_der_gwdg

Further information and useful tips on the subject of security on the Internet can also be found here:

- http://www.bsi-fuer-buerger.de

XI. Usability of the voting system despite technical or personal limitations
As a matter of principle, the election application is accessible to all authorised users, irrespective of their physical and / or technical capabilities, largely without restriction, without any particular difficulties and in the generally accepted manner, and can generally be used without assistance (barrier-free). This includes both the use by persons with and without health impairments, as well as the use with technical restrictions (e.g. text browser or PDA). The information presented can be read aloud using special computer programmes (screen readers) or output in Braille for blind and visually impaired persons with the appropriate aids.

XII. Voting system
The POLYAS voting system of POLYAS GmbH (www.polyas.de) is used for the online election. The voting system consists of three technical modules. The electoral roll module contains an anonymous register, which only contains the voting numbers and no personal data. The separate module Electoral Release (Validator) grants the possibility to vote and the equally independent module Ballot Box is used for the storage and counting of votes. The internet is used as the transmission channel for online voting. The communication between the modules is exclusively encrypted using the "https" protocol, which is considered to be sufficiently secure. Data that could indicate the personal identity of eligible voters are NOT stored in the voting system. The security of the servers used for the operation - which work strictly separately - as well as the procedures used there are guaranteed by the technical operators according to generally recognised security standards.

XIII. Authorisation via a university user account
Those entitled to vote register by entering their matriculation number and password (of the University user account) via the University's election portal at https://onlinewahl.uni-goettingen.de/onlinewahl. After logging in, the system checks whether the user is entitled to vote and then generates a temporary URL (SecureLink) to the voting system. No further login to the voting system is necessary; the eligible voters can start voting directly. The identity of the voter is protected.

XIV. Logging out of the voting system / Automatic time monitoring /
If you wish to cancel or interrupt the voting process, please exit the voting system in the correct manner by clicking on the "Cancel/logout voting" button (above). If you have logged in and been inactive for 15 minutes, you will be logged out automatically. This is for the security of your vote; of course, your previous vote selection will not be (temporarily) saved in this case. You can log in again within the voting period and vote digitally.

XV. Postal voting
An application for a postal vote could be submitted to the election administration until 02 January 2024; 15:00 (cut-off time). Once the postal voting documents have been sent or handed over, eligible voters are excluded from online voting.

XVI. Assistance in case of problems and questions
You will find instructions or assistance on how to conduct the election process on the website: www.uni.goettingen.de/wahlen. For more in-depth questions, detailed voting instructions are also available online in the voting system.

If you notice a security-relevant irregularity, e.g. a manipulation, please contact the university's election management immediately.

XVII. contact information
If technical problems or questions should arise in relation to your personal EDP terminal, please contact directly the persons responsible for the computer network to which the EDP terminal you are using is connected.

Contact:
Election Administration of the Georg-August-Universität Göttingen
Department of Academic Law and Sponsoring Foundation
Section 81
Von-Siebold-Strasse 2
37075 Göttingen
https://www.uni-goettingen.de/wahlen

Contact person:
Ralf Buhre
ralf.buhre@zvw.uni-goettingen.de
Tel. +49 551 39-28093