# SINGAPORE TABLE TENNIS ASSOCIATION
# INFORMATION TECHNOLOGY (IT) POLICY

Approved by the Management Committee on 11 Feb 2025

| | |
|---|---|
| **1** | **PURPOSE** |
| 1.1 | IT policy defines the rules, regulations, and guidelines for the proper usage, security, and maintenance of the STTA's technological assets including the computers, mobile devices, servers, internet, applications, etc. It establishes guidelines for the acceptable and ethical use of the company's IT infrastructure to ensure the safety, security, and integrity of the data, products, and/or services used by the company as well as of those offered to its customers. |
| **2** | **SCOPE OF THE POLICY** |
| 2.1 | Users<br>The policy is applicable to employees of STTA who are given access to its server and device, its IT partners, IT vendors and any other persons who are given access to its IT resources. These are referred to as "Users" hereinafter. |
| 2.2 | Devices<br>The devices that the policy covers include:<br>• STTA's computers including desktops and laptops<br>• STTA's servers<br>• STTA's CCTV and network<br>• STTA's Printers and scanners<br>• STTA's iPads and handphones<br>• Any other device, whether or not it belongs to STTA, with information-handling technology used for STTA related business and activities |
| 2.3 | Applications and tools<br>The policy covers applications and tools such as, but not limited to:<br>• STTA email accounts<br>• ABSS accounting software (MYOB) and any new accounting software that STTA uses<br>• Microsoft application software, including but not limited to, MS Word, MS Excel, MS Power Point<br>• Adobe Acrobat<br>• Workfloww and any other HR software applications<br>• Tournament software<br>• Membership system<br>• Any other software used by the users that are installed on or connected to STTA's device<br>• Software installed on personal device that are used for communication with STTA or access to STTA's server or device |
| 3 | **PURCHASE AND INSTALLATION GUIDELINES** |
| 3.1 | The purpose of purchase and installation guidelines is to ensure that all hardware and software used are appropriate, provide value for money, and integrate with |

| | |
|---|---|
| | other technologies used within the organization. Another important objective of the purchase policy is to ensure that there is minimum diversity of hardware as well as software within the organization. Uniformity in the devices and software ensures ease of maintenance and IT support. |
| 3.2 | <u>For use by High Performance</u><br>The High-Performance Manager shall assess the needs required for high performance and evaluate with the IT vendor, internally with the users and the CEO. The result will be proposed for approval based on the Financial Policy before purchase is carried out.<br><br><u>For use by all other employees</u><br>The FCS department, upon receiving request from the users, shall evaluate, propose and seek approval for the purchase. The evaluation may include communication with the IT vendor and internally with the users and the CEO.<br><br>The above processes are to ensure that there is uniformity in the devices and software for the ease of maintenance and IT support. |
| 3.3 | Before a device or software is purchased and installed, the proper approval and procurement procedures set out in the Financial Policy must be adhered to. |
| 3.4 | Installation of software application is restricted to User with Administrator access rights, which is outsourced to the authorised IT Vendor. |
| 3.5 | **Device User Maintenance** list containing user's name, ID, date entrusted with the device, shall be maintained by the FCS Executive or his/her covering Officer and reviewed by FCS Manager **whenever there is user turnover**. In addition, the updated list shall be approved by the CEO on a yearly basis. |
| 3.6 | The maintenance and support on IT solutions is by the IT Vendor engaged by STTA. |
| 3.7 | For software or systems that are developed and customised to STTA's needs, the process also includes user testing before it is installed and/or go live. |
| 4 | **<u>USAGE POLICY</u>** |
| 4.1 | The usage policy sets the guidelines for the allocation, usage, and maintenance of all company-owned equipment, data, and technology. It defines the guidelines that are important for every user to have an understanding on how he/she is to use the STTA's technological resources responsibly, safely, and legally. |
| 4.2 | Users have the responsibility to utilise the STTA's IT Resources properly for purposes consonant with the mission of the STTA and in accordance with all Singapore laws, whether they are within STTA or remotely or overseas. |
| 4.3 | Files that are used in the cause of official business are the property of STTA. The access and ability to alter another user's files does not in itself imply the permission to alter those files.<br><br>Under no circumstances may a user alter a file that does not belong to him or her without prior permission of the file's owner or of STTA. |

| | |
|---|---|
| 4.4 | Security is the responsibility of all users. STTA shall conduct regular cybersecurity and data protection awareness briefings for /via emails to users who are given access to STTA's IT resources. |
| 4.5 | A user is not permitted to allow third party any access to STTA's IT Resources without prior written consent from the CEO of STTA or his/her designee. In addition, a user is not permitted to transfer or sell/resell resources/materials sourced from STTA's IT Resources to third party whether or not a fee or any other forms of payment-in-kind is given in return. |
| 4.6 | **Deleting Electronic Communications**. Users of the STTA's IT Resources, particularly its email system should be aware that electronic communications are not necessarily erased from the computer system when the user "deletes" the file or message. Electronic communication may continue to be stored on as a backup copy long after it is "deleted" by the user. |
| 4.7 | **Inspection of electronic Information**. Information located on STTA's IT Resources may be subject to examination, as and when deemed necessary, to maintain or improve functioning of technology resources, investigate alleged violations of STTA policies and/or Singapore law and/or the relevant local laws applicable to any foreign countries the user is in located. |
| 4.8 | In **disciplinary proceedings**, STTA, at its discretion, may submit results of investigative actions to authorised personnel and/or law enforcement agencies. Information and communications created with/communicated through STTA's IT Resources may be subject to legally binding demands, such as court orders. Ultimately, it is STTA that owns the IT resources and all information and communications created through them, not the users who use them. |
| 4.9 | **Right of STTA Access.** STTA reserves the right for authorised personnel to access a user's stored information to investigate suspected cases of computing abuse and for systems maintenance purposes. Such access shall be approved by the CEO of STTA or his/her designee and in consultation with the Disciplinary Committee, President and/or the Management Committee where necessary. |
| 4.10 | **Security and Privacy.** STTA employs various measures to protect the security of its information technology resources and of user data and accounts. Users may have a reasonable expectation of unobstructed use of information technology resources, certain degrees of privacy, and protection from abuse and intrusion. However, security precautions cannot always guarantee users security or privacy. Users should exercise caution in using STTA's IT Resources, especially when storing and/or transmitting confidential data. **Password protection is necessary for confidential files. Password should be sent in a separate email, without the file attached, to the party receiving the confidential file.** |
| 4.11 | **Disclaimer.** STTA accepts no responsibility for any damage to or loss of data, hardware, or software arising directly or indirectly from the use of STTA's IT resources or for any consequential loss or damage. STTA makes no warranty, express or implied, regarding the facilities offered or their fitness for any particular purpose. |
| 4.12 | **<u>Specific Prohibitions on Use</u>**<br><br>The following categories of use are inappropriate and prohibited: |

| | |
|---|---|
| 4.12.1 | **Use that attempts to damage the integrity of STTA or other IT Resources**. |
| a) | STTA's IT Resources may not be used for making unauthorised connection to, monitoring of, breaking into, or adversely affecting the system's performance, whether these system(s) belong to STTA or not. The ability to connect to other systems via the network does not imply the right to use or connect to them unless given proper authorisation by the system owners. |
| b) | Users must not steal or attempt to use methods of electronic or any means (e.g., software, hardware, or firmware) to eavesdrop on passwords, content, and information that he/she is not authorised to access. |
| c) | STTA's IT Resources shall not be used to access, transmit, store, display, or request for inappropriate content such as obscene, pornographic, erotic, profane, racist, sexist, defamatory or offensive materials. |
| 4.12.2 | **Use that impedes, interferes, or otherwise causes harm to activities of others.** |
| a) | Users must not engage in any actions that may interfere with a system's supervisory or accounting functions, cause network congestion, or interfere with the work of others. Examples of prohibited conduct include placing unlawful information on the system, the transmitting of data or programmes likely to result in the loss of recipient's work or system downtime, sending of "chain letters" or "broadcast" messages to lists or individuals, or spamming or gaming via the STTA network. |
| b) | Users must <u>not</u>:<br>• develop and/or use programmes that may harass or harm other users of the system;<br>• develop and/or use programmes that may attempt to bypass system security mechanisms, or to steal passwords or data;<br>• develop and/or use programmes that, by design, attempt to consume all of an available system resource;<br>• develop or use programmes designed to replicate themselves or attach themselves to other programmes, commonly called "worms" or "viruses"; or<br>• develop and/or use programmes designed to evade software licensing or copying restrictions. |
| 4.12.3 | **Use in Violation of the Law.** |
| a) | **Unauthorised Access or Use**. It is a violation to use another person's account, with or without that person's permission. Users should use only the computer accounts they are individually authorised to use. |
| b) | Users should not attempt to crack, guess, or otherwise capture another person's computer or account password. |
| c) | **Disguised use**. Users must not conceal their identity when using STTA's IT resources, except when the option of anonymous access is explicitly authorised. Users are expressly prohibited from masquerading as or impersonating others or otherwise using a false identity. |
| d) | **Use in Violation of Laws**. Users must not use their STTA's account and IT resources in any way that violates the laws of any country. STTA expects its users to be cognisant with and to abide by the provisions stipulated in the Computer |

| | |
|---|---|
| | Misuse Act (Chapter 50A) and Cybersecurity Act 2018 and the Sedition Act (Chapter 290). This applies to all STTA users, including while overseas and not within STTA premises. |
| e) | **Copyright.** Users are responsible for ensuring that no copyrighted material (including music, film, podcasts, books, games, and/or software) is downloaded using, published on, or distributed from STTA's network without the copyright holder's permission. Users should be aware of the Copyright Act 2021 and the Digital Copyright Policy in force. Users are also to note that in some instances and depending on the type of content, they may be subjected to the laws of a foreign jurisdiction. |
| f) | **Personal Data Protection Laws**. Users are responsible for ensuring that the collection, use, and disclosure of Personal Data are in compliance with Singapore's Personal Data Protection Act 2012 (PDPA). Generally, users should obtain valid consent before they collect, use, or disclose Personal Data, unless any exception applies.<br><br>The STTA **Personal Data Privacy Policy** (PDPP) in Appendix A shall be referred in conjunction with this policy. |
| 4.12.4 | **Use in Violation of STTA Contracts.** |
| a) | **Copyrighted Materials and Licensed Software, Programmes and Data.**<br>Users must:<br>• not transfer, duplicate, make available or obtain illegally, any copyrighted material including, but not limited to, agreements, license software, programmes, and data;<br>• respect the rights of others by complying with all STTA policies and the relevant local law regarding intellectual property;<br>• not install unlicensed or unauthorised software in the local (meaning desktop / laptop / computing devices) hard disk or on any server drives of STTA. |
| b) | **Guidelines from Third-party or subscribed services.** When accessing other organisations' IT facilities and resources from the STTA's network, users are responsible for abiding by these terms and conditions, relevant local laws, and the relevant policies of such other organisations. |
| 4.12.5 | **Use in Violation of STTA Policies.** |
| a) | The privilege of using STTA's equipment, including the network cabling, wireless access, computer and network systems and servers, broadcast media, and access to global communications and information resources is provided and granted by STTA, and may not be transferred or extended to people or groups outside the STTA, without prior authorisation. |
| b) | **Email and Web Policies**.<br>Users must manage the use of email and web pages in accordance to the guidelines below. As a general guidance, the following conduct / actions are prohibited:<br>• harassing, sending pornographic or defamatory materials / messages via e-mail or through posting to Web pages;<br>• sending or posting forged email ("masquerading"), web pages and/or newsgroups or chat group messages; |

| | |
|---|---|
| | • massive or unsolicited emailing without explicit approval;<br>• flooding a user or a site with very large or numerous pieces of email; and<br>• sending or forwarding of confidential STTA information via email and any other media.<br><br>Offenders will be held liable and sanctioned accordingly, depending on the severity and to be assessed by the management of STTA. At the discretion of the STTA's management, it may be escalated to the Disciplinary Committee and Management Committee for disciplinary action to be carried out. |
| 4.13 | **Responsible and Acceptable Use** |
| a) | **Personal Account Responsibility.** Accounts are assigned to individuals and are not to be shared unless specifically authorised by the management of STTA. Users are solely responsible for all functions performed from the accounts assigned to them. |
| b) | **Not allowing others to use individual's account.** Users should safeguard their computer accounts and passwords. Peer pressure and/or negligence cannot be accepted as a defence of wrongdoing or misconduct. |
| c) | Users are responsible for ensuring the absolute privacy and secrecy of their accounts and passwords by:<br>• changing any pre-assigned default password at the first possible opportunity;<br>• avoiding composing passwords based on their personal information (e.g., name, user ID, date of birth, etc).<br>• set password with at least 8 alphanumeric characters with at least 1 special character, 1 upper and 1 lower case.<br>• changing password yearly as prompted by the system. |
| d) | **Remote use** to access STTA's server will require the user to log in to VPN, using his/her VPN ID and 2FA (password and OTP sent to the user's email). The User should not share his/her password with any other person or entity. |
| 4.14 | **Responsibility for safeguarding STTA's IT Resources.** Users should actively protect and defend STTA's IT Resources against unauthorised access and use. |
| a) | Users should have the anti-virus software running on their laptop/PC and update the anti-virus signature file whenever prompted. |
| b) | When prompted by the device, users should update the operating system (OS) and other networked devices, including mobile phones and iPads where applicable. |
| c) | User should switch the laptop/PC to lock screen mode whenever not in use or away from the device. This is to prevent unauthorised use and unauthorised access to information in the device.<br><br>User should turn off the laptop/PC at the end of the day before leaving office or at least once a week. The former is to allow the device to be updated when prompted before turning off and prevent overheating. Laptop should be kept under lock to prevent loss. |

| | |
|---|---|
| d) | When user, who is an employee, leaves STTA's employment, he/she will need to return all assets, including IT resources, under his/her custodian. The HR cessation procedure shall be followed to ensure that all resources are returned to STTA. |
| 4.15 | **Backup.** All data on the STTA server systems is subject to backup at the sole discretion of STTA. While STTA will do its utmost efforts in ensuring the integrity of the backed-up data, STTA cannot guarantee that all backed-up data can be restored. Users therefore have the responsibility to backup their own critical files and systems.<br><br>Users are responsible for the backup of their files saved on their desktop as these are not backed up at Association's level. Hard disks / thump drives are provided to users for their back up. Users need to **keep all the STTA's IT resources under lock**, especially those that contain confidential or sensitive data. |
| 4.16 | STTA provides IT resources and services to its users for its business use. **Prohibited use** of these resources, whether on STTA's premises and remotely includes, but is not limited to, political campaigning, solicitation, unauthorised financial gain, or conducting any business that has no official relationship with STTA. Additional limits may be imposed by a supervisor, CEO, the Management Committee, applicable STTA policies and/or Singapore laws and/or the relevant local laws. |
| 5 | **POLICY ENFORCEMENT** |
| 5.1 | **Use is Revocable.** The use of software, databases, and/or computer and network resources at STTA is a revocable privilege. All users are responsible for using these resources and facilities in an effective, ethical, and lawful manner. The use of STTA's IT Resources has been made available for the purpose of supporting the business and operations in STTA only. |
| 5.2 | **Disciplinary measures** for violation are normally applied by the Management, CEO, Disciplinary Committee and the Management Committee. Violators may be subject to additional penalties and disciplinary actions by STTA and are also subject to international and Singapore laws governing interactions that occur on information technology systems and the Internet. STTA may restrict or deny access to information technology resources temporarily or permanently, including prior to the initiation or completion of investigation and disciplinary procedures, when it appears necessary to protect the integrity, security, or functionality of STTA's IT resources. |
| 5.3 | **STTA's right to Indemnity**. Failure by users to observe the policy may also result (directly or indirectly) in STTA being involved in claims and/or suffering damages, losses and expenses. The user shall indemnify STTA and its officers from such claims, damages, losses, and expenses resulting from the user's intentional failure to observe the policies. In addition, the user must understand that STTA will cooperate in any official investigations in Singapore or any other relevant jurisdiction resulting from any breach of these policies and may, at its discretion, decide to furnish the relevant authorities/parties with the relevant information and user's consent to any such disclosure shall be deemed by all users' acceptance of this policy. |
| 5.4 | **Waiver.** When restrictions in the policies interfere with the operation of STTA, user may request for a written waiver from the CEO or his/her designee. |

| | |
|---|---|
| 6 | **ROLES AND RESPONSIBILITIES** |
| 6.1 | **All Users** of STTA's IT Resources have an obligation to report any misuse of STTA's IT resources or suspected breaches of conditions in IT policy to the management of STTA. |
| 6.2 | The **FCS department** shall investigate and manage all breaches or suspected breaches of the IT policy in accordance with the guidelines in this policy. |
| 6.3 | External **IT Vendor** shall:<br>• Provide the technology support for investigating infringements or alleged breaches of this policy; and<br>• If necessary, to temporarily block the user from accessing STTA's IT Resources if his/her continuous access is detrimental to the Association. |
| 6.4 | After investigation is completed, the matter will be reported to the **CEO** for a decision on whether further escalation to the higher authority is necessary based on the severity of breach. |
| 6.5 | If the case is escalated to the **Disciplinary Committee** (DC), the DC shall assess and decide on an appropriate disciplinary action against the defaulting user. |
| 6.6 | Approval will subsequently be obtained from the **Management Committee** before the disciplinary action is carried out and / or conclusion and decision is conveyed. |
| 7 | **REGULAR UPDATES** |
| 7.1 | Regular updates on IT, Data Security and Cyber Security shall be sent to users by the FCS Department or Data Security Officer or the STTA management. |
| 7.1 | Updates will also be communicated via training / briefing by IT Vendor(s) and or email from the IT Vendor(s). |

**Appendix A**

**Singapore Table Tennis Association (STTA)**
**Personal Data Privacy Policy**
**(Approved by Management Committee on 11 Feb 2025)**

In this Personal Data Privacy Policy, the words "STTA", "we" and "us" refer to the Singapore Table Tennis Association. It is located at 5 Stadium Drive #03-40, OCBC Arena, Singapore 397631.

## BACKGROUND

In view of the enactment of the Personal Data Protection Act effective from 2 July 2014, STTA has put in place a personal data privacy policy in relation to collection, use, disclose and/or process your child/children and/or your personal data in dealings with STTA.

Personal data means information about your child/children or you, whether true or not, set out in your child/children applications, registration forms and documents and any other personal information voluntarily provided by you and processed by us. Some examples are, but not limited to, name, age, citizenship, identification number, academic status and results, medical and disability information, residential address, mobile and residential telephone number, personal email address, bank account, photograph or video image and etc.

## PURPOSE

STTA will/may collect, use, disclose and/or process your child/children and/or your personal data for one or more of the following purposes:

(a) Processing your child/children admission/registration application with us;

(b) Administering, processing and/or managing your child/children application(s) for awards, scholarship (whether such award or scholarship is provided by the STTA or any third party) and/or financial assistance, grants or bursaries, and if successful, administering and/or managing your child/children awards, scholarships and/or financial assistance, grants or bursaries;

(c) Supporting and/or dealing with your child/children trainings, competitions, health, medical needs, safety and welfare requirements such as but not limited to athlete support services.

(d) Administering and/or managing activities, events and competitions organised and/or held by STTA. Please do note that photographs(s) or video images of your child/children and/or you may be taken during such activities/ events/ competitions and used, disclosed, processed and published on STTA & co-organisers' social media platforms, websites and in materials such as publications, or any materials/books and you agree to the same;

(e) Administering and/or managing the use of training facilities;

(f) Contacting your child/children and/or you via different modes such as phone/voice call, short text message, email and/or postal mail for STTA related matters such as but not limited to STTA events, training, competition arrangement and fees communicating with your child/children and/or you in the event of public transport disruptions, emergencies or other extraneous circumstances such as national disasters, health pandemics, fire drills, evacuation drills and etc.;

(g) Carrying out background checks, investigation and screen activities in accordance with legal or regulatory obligations that may be required by the Singapore law or that may have been put in place by us;

(h) Dealing with complaints related matters;

(i) Conducting disciplinary and security matters and/or arrangements. Please be informed there are surveillance cameras installed in STTA for security reasons;

(j) Producing statistics and research for internal and/or statutory reporting and/or record keeping requirements and performing STTA policy/process reviews;

(k) Carrying out research, analysis and development activities, including but not limited to data analytics, surveys and/or profiling to improve any of the STTA programmes:

(l) Responding to requests for information from local hospitals, embassies, public agencies, ministries, statutory boards or similar authorities;

(m) Complying with any government or regulatory requirements of any relevant jurisdiction to make disclosure;

(n) Maintaining and promoting your child/children alumnus relationship with us by informing your child/children and/or you, but not limited to, of activities, events and updates to the STTA's development by phone/voice call, short text message, email and/or postal mail and by providing your child/children and/or you with STTA's publications that are for alumni;

(o) Conducting publicity and/or the development of promotional materials to showcase and market your child/children achievements as an athlete and/or alumnus of STTA, publishing your child/children and/or your image and/or personal data on public media platforms. The STTA has the right to use your child/children and/or your name, photograph, video images, personal story and information you provide to STTA in the STTA's promotional materials;

(p) Contacting your child/children and/or you for fund raising activities for STTA selected causes by various modes of communication platforms including but not limited to phone/voice call, short text message, email, social media and/or postal mail;

(q) Processing, administering, preparation and compilation of any documents relating to your involvement in STTA, as well as for all statutory filing and submission compliance, if required;

(r) Contacting you and for dissemination of information with regards to your involvement with STTA, whether as a volunteer or donor;

(s) Processing and administering the donations you made to STTA.

**CONSENT TO THIRD PARTIES**

Photograph(s) or video image(s) of athletes and/or their parents/guardians may be captured during the STTA's activities/ tournaments/trainings and events. The Association may use and publish such photographs and/or video recordings in the Association's publications, website, social media channels, and other communication channels.

**DISCLOSURE TO THIRD PARTIES**

The STTA may be required to disclose your child/children and/or your personal data to third parties which would be processing your child/children and/or your personal data for one or more above purposes. These third parties include but not limited to the following:

(a) Organisations such as but not limiting to tournament co-organizers with which we are collaborating for one or more of the abovementioned purposes;

(b) Individuals, Organisations and/or any government authority who have provided your child/children with scholarships, financial assistance, awards, medals or prizes during the period of your child/children trains in STTA and who request for information relating to your child/children progress and result as a trainee/athlete in STTA;

(c) Any service providers engaged by the STTA who process your child/children and/or your personal data on behalf of the STTA including but not limited to hospitals, medical centre(s), training institutions and those which supply administrative services to the STTA such as manufactures of award medals, plagues, trophies, information technology companies and printers of the STTA publications;

(d) Organisations and/or table tennis institutions which are involved in exchange programmes with us;

(e) Organisations, Grantor and/or any Government Authority, for the administration and statutory compliance of your donations made to STTA;

(f) STTA's agents, service providers, Grantor and/or Government Authority for publishing, disclosure and/or reporting compliance.

We may/would not be able to process your child/children with us for place and/or financial assistance, grants and/or bursaries whether they are from us or external organisatons should you fail to supply us certain personal data. Likewise, the STTA may/would not be able to effectively administer our relationship with your child/children and/or you.

The STTA will not disclose any extend greater than necessary which we determine in good faith.

**ACCESS, UPDATE, CORRECTION AND WITHDRAWAL**

You have the right to request access to, update and/or correct your child/children and/or your personal data held by us. If you wish to do so, please contact our STTA Office and provide details of your access, update and/or correction request.

You may withdraw your consent given, whether in part or as a whole. Depending on the degree of your withdrawal of consent for us to collect, use, disclose and/or process your child/children and/or your personal data, we may not be able to administer process and/or manage your child/children and/or your existing relationship with us. Should you wish to withdraw your consent in part of whole, please send an email to our tabletennis@stta.org.sg and provide details of your withdrawal request.

**QUERIES**

If you have any questions relating to our collection, use, disclose and/or process of your child/children and/or your personal data or the matters set out in this document, please contact our STTA Office.

**FREQUENTLY ASKED QUESTIONS**

<u>Access and Correction</u>

1) Can I request to correct my personal data held by STTA?

Yes, you can. You have the right to correct an error or omission in your personal data which STTA holds. If you wish to do so, please contact our STTA Staff at tabletennis@stta.org.sg and provide details of your correction request.

<u>Care of Personal Data</u>

2) How long my personal data can be retained by STTA?

The PDPA does not prescribe the retention period. STTA will however cease to retain your personal data when there is no longer necessary for business or legal purposes.

3) Can I ask STTA to delete my personal data from their records?

You can ask STTA to stop collecting, using, processing and/or disclosing your personal data in part or in full at any time. STTA is however not obliged to delete it and may retain it for business and legal needs.

**APPENDIX B**

# STTA IT POLICY
# USER ACCEPTANCE FORM

I have read, understood, and accepted the IT Policy, in particular clause 4 on the Use of IT resources set out in the policy, including any future revisions to the same.

| | |
|---|---|
| Name: | |
| Username issued: | |
| Date: | |
| Signature: | |