



STUDENT CONTRACT

This contract governs the relationship between STU and students enrolled in distance learning courses in conjunction with the University's General Regulations, published on the STU institutional website.

FOREWORD

STU is a nonprofit entity and, in compliance with the statutory and organizational autonomy recognized to universities in general, has the power to determine autonomously, through its regulatory activity, the tuition fee and university contributions for all courses of study activated.

The amounts charged to students by specific fees or contributions do not represent a consideration for opposing services but an individual contribution to covering the cost of services offered by the University to realize the above purposes.

The STU's website publishes all amounts with payment methods and exemption cases.

ARTICLE 1 - NATURE AND PURPOSE OF THE CONTRACT

This contract, the preamble to which is an essential part, represents the formal act by which the student adheres to the services offered by the distance learning course of their choice, which St. Thomas University provides in compliance with the general requirements and specific requirements contained in the Catalog and the General Regulations of the University, both of which are published on the University's website.

The contract also regulates how the relationship may be terminated at the student's request and guarantees the completion of their education.

ARTICLE 2 - GUARANTEE TO THE RIGHT TO STUDY

The University guarantees the right to study of every student enrolled in its distance learning courses, committing itself to organize and provide educational services by the methods, curricula, and rules established in the Service Charter and to respect the teaching methodology adopted and the service levels offered.

STU guarantees that the teaching material has been certified by a special committee composed of faculty members and that the student's evaluation will occur through its verifications. The examinations are generally held at the University's premises unless an exception is made.

STU issuance of degrees by committing to maintain the standards set by accreditation for distance learning according to the criteria, requirements, and procedures

ARTICLE 3 - DESCRIPTION OF SERVICES AND GUARANTEE OF USABILITY

The University undertakes to provide online educational activities. It supports the student about the distance learning course chosen by the latter, described in the Student Services and the Policies for the Management and Use of Educational Services for Information Technology, Educational Services, Information Services, Tutoring Services, Intelligent Library Services, Orientation Services, Administrative Secretarial Services, and Research Services.

The University guarantees maximum flexibility in distance learning courses, allowing the student to select the maximum number of annual credits that can be earned and dilute these credits over a multi-year scope.

The University guarantees access to educational services to students with disabilities, committing to adopt the measures provided in the University Teaching Regulations and the Service Charter and keep them updated according to technological standards.

The university keeps online educational activities and supports usability systematically, continuously, and without interruption.

ARTICLE 4 - DESCRIPTION OF TECHNOLOGICAL SOLUTIONS AND GUARANTEE OF USABILITY

The student has access to the educational services, training, and information support of the chosen distance learning course through the following tools: Interactive classroom, e-learning platform, and web portal.

The University guarantees that these tools are characterized by the following:

- a. the use of network connection for the benefit of learning materials and the development of educational activities based on interactivity with teachers/tutors and other students
- b. the use of the student's personal computer, possibly supplemented by other interfaces and devices as the primary tool for participation in the learning process
- c. a high degree of independence of the learning path from constraints of physical presence or specific timetable
- d. the use of standard, interoperable, and modularly organized learning content that can be customized concerning the characteristics of end users and delivery paths
- e. continuous monitoring of the level of learning, both through path tracking and frequent moments of evaluation and self-assessment.

ARTICLE 5 - UNIVERSITY FEES AND OTHER CONTRIBUTIONS, EXEMPTIONS, AND WAIVER OF STUDIES

At the beginning of each academic year, the University determines the University Tuition and Fees and other contributions due by the student for the chosen course of study.



The student must pay the University Tuition and Fees and other contributions: annual enrollment in the degree program, transfer to another university, graduation, and information of need on STU's website.

A student who is late in payment cannot be admitted to the next course, nor can they obtain any certificate related to their educational career in the part to which the late payment refers, nor can they get permission to transfer to another university. No refund will be given for unofficial withdrawal or dismissal from STU.

Students enrolled who withdraw before the start of the course(s) will be entitled to a refund of 100% of the tuition paid.

Students enrolled who withdraw in the first and second week of the course will be entitled to a refund as per the table below:

Before the 1 st week	100%
1 st week	50%
2 nd week	30%
After the 2 nd week	0%

Administrative and Resources fees are non-refundable unless prohibited by some provision of law. A student who withdraws from a course will have access to the electronic course materials at no additional cost if the student re-enrolls within 180 days of the withdrawal date.

Students enrolled in one or more courses after the second week of the course will be responsible for full payment and will not be entitled to any refund.

Reimbursements do not include bank fees incurred and are not the responsibility of STU.

The student, at any time, may terminate the contractual relationship with the University by notifying the secretary of their renunciation of studies.

Renunciation results in the loss of the student's status and extinguishes their career without prejudice to the credits acquired; therefore, the student may obtain the certificate for their previous job, duly pursued, supplemented by the annotation attesting to the renunciation of studies.

ARTICLE 6 - INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY

All individuals granted access to or use of University Resources must be aware of and agree to abide by the following acceptable use requirements:

A. Definitions

STU: St Thomas University

University Information Resources: All computer and telecommunications equipment, software, data, and media, owned or controlled by the University or maintained on its behalf.

University Data: All data or information held on behalf of the University, created as a result and/or in support of university business, or residing on University Information Resources, including paper records.

Confidential Data or Confidential Information: All University Data that is required to be maintained as private or confidential by applicable law(s).

User: Any individual granted access to University Information Resources.

B. General

1. University Information Resources are provided to conduct the University's business.
2. Users have no expectation of privacy regarding any University Data residing on University-owned computers, servers, or other information resources owned by, or held on behalf of, the University. Additionally, users must also understand and accept that they have no expectation of privacy in any personal information stored by a User on a University Information Resource, including University email accounts. The University may access and monitor its Information Resources for any purpose consistent with the University's responsibilities, duties, and/or mission without notice.
3. Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device.
4. All Users must comply with applicable University Information Resources Use and Security policies, procedures, and standards at all times.
5. Users shall never use University Information Resources to deprive access to individuals otherwise entitled to access University Information Resources, to circumvent University computer security measures, or in any way that is contrary to the University's mission(s) or applicable law(s).
6. Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of the University and is approved in writing by the President or a specific designee. The viewing, access to, storage, or transmission of sexually explicit materials as Incidental Use is prohibited.
7. Users must clearly convey that the contents of any email messages or social media posts that are the result of Incidental Use are not provided on behalf of the University and do not express the opinion or position of the University. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, St Thomas University."
8. Users should report misuse of University Information Resources or violations of this policy to their supervisors or through an approved reporting format.



C. Confidentiality & Security of Data

1. Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not authorized to access. Users shall maintain all records containing University data by the University's information and data security policies, procedures, and standards, as well as the Records Retention Policy and Records Management Guidelines.
2. Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official University duties.
3. Whenever feasible, Users shall store Confidential Information or other information essential to the mission of the University on a centrally managed server or University approved storage location rather than a local hard drive or portable device.
4. In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device, such as a laptop computer, tablet computer, or smartphone, the User must ensure the data is encrypted and secured by the university and any other applicable requirements.
5. The following University Data must be encrypted during transmission over an unsecured network: Social Security/National ID Numbers; personally identifiable Medical and Medical Payment information; Driver's License Numbers and other government-issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other University Data about an individual likely to expose the individual to identity theft.
6. Users who store University Data using Cloud services must use services provided by or sanctioned and approved by the University through the approved University services rather than personally obtained Cloud services.
7. Users must not use security programs or utilities, except as such programs are required to perform their official duties on behalf of the University. The use of security programs or utilities must be approved, in writing, by the University's Chief Information Security Officer.
8. To help ensure the proper security of University Resources, all computers or other electronic devices connecting to a University network must run up-to-date operating systems, patches, and security software as prescribed by the Information Security Office.
9. Devices determined by the University to lack the required security standards or software or to otherwise pose a threat to University Information Resources may be immediately disconnected from a University network or service without notice.

D. Email

1. Emails sent or received by Users while conducting University business are University Data that is subject to records retention and security requirements.
2. Once provided, Users are to use university-provided email accounts, rather than personal email accounts, for conducting University business.
3. The following email activities are prohibited when using a University provided email account:
 - a. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.
 - b. Accessing the content of another User's email account except 1) as part of an authorized investigation, 2) as part of an approved monitoring process, or 3) for other purposes specifically associated with the User's official duties on behalf of the University.
 - c. Sending or forwarding any email that the User suspects to contain computer viruses or malware.
 - d. Any Incidental Use prohibited by this policy.
 - e. Any use prohibited by applicable University policy.

E. Incidental Use of UTRGV Information Resources

1. Incidental Use of University Information Resources must not interfere with the User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University policies.
2. Users must understand that they have no expectation of privacy in any personal information stored by a User on a University Information Resource, including University email accounts.
3. A User's incidental personal use of University Information Resources does not extend to the User's family members or others, regardless of where the University Information Resource is physically located.
4. Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited.
5. Incidental Use for purposes of political lobbying or campaigning is prohibited.
6. Storage of any email messages, voice messages, files, or documents created as Incidental Use by a User must be nominal (less than 5% of a User's allocated mailbox space).
7. Files unrelated to University business may not be stored on network file servers.

F. Additional Requirements for Portable and Remote Computing

1. All electronic devices including personal computers, smartphones, or other devices used to access, create, or store University Information Resources, including email, must be password protected and passwords must be changed



whenever there is suspicion that the password has been compromised.

2. Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted and follow all prescribed University policies, procedures, and standards.
3. University Data created and/or stored on personal computers, other devices, and/or non-university databases should be transferred to University Information Resources as soon as feasible.
4. All remote access to networks owned or managed by the University must be accomplished using a remote access method approved by the University, as applicable.

G. Password Management

1. University-issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e., Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.
2. Each User is responsible for all activities conducted using the User's password or other credentials.

ARTICLE 7 - STUDENT'S COMMITMENT

The student, for the achievement of their educational and professional goals and within the framework of the chosen study plan, commits themselves to full compliance with the rules of the University Teaching Regulations, the teaching regulations and orders, the general student rights and duties regulations, as well as the Catalog published on the institutional website. The student must complete the "Student Opinion" questionnaire at the end of each course. Submission of the questionnaire is a mandatory condition. The University guarantees that the data will be used anonymously.

The student agrees to attend lectures, tutorials, seminars, and, in general, all educational activities organized by the University for the program-base of the Course of Studies.

Students who have interrupted their studies without formally renouncing them may not enroll in another university.

ARTICLE 8 - DURATION

The duration of this contract is equal to the student's stay at STU until the completion of the course of study or its discontinuation.

The academic year starts from the day of the first enrollment and lasts one calendar year.

User Acknowledgment

Signature: _____ Date: _____

Print Name: _____