Turkish Journal of Computer and Mathematics Education Vol.12 No.6 (2021), 5381-5389

Research Article

A Zero-Trust Model-Based Framework For Managing Of Academic Dishonesty In Institutes Of Higher Learning

Atiff Abdalla Mahmoud Arabi[a], Aduragbemi David Ogundijo[b], Tadiwa Elisha Nyamasvisva[c]

[a,b] Center for Postgraduate Studies and Research (CPSR)
[c] Faculty of Engineering, Science and Technology (FEST)
[a,b,c] Infrastructure University Kuala Lumpur, Unipark Suria, Jalan Ikram-Uniten, 43000 Kajang, Selangor Darul Ehsan, Malaysia.
[a]202922056@s.iukl.edu.my, [b]153916199@s.iukl.edu.my, [c]tadiwa.elisha@iukl.edu.my

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: As Academic dishonesty has become one of the most disturbing problems in many Institutions of higher Learning (IHLs) across the globe [1],[2], it has been noticed that this behavior will lead to an unfair atmosphere of competition among the students[3]. As part of a larger study on academic dishonesty, this paper aims to explore the effective countermeasures towards academic dishonesty and propose a framework for the prevention of academic dishonesty in IHLs based on the Zero Trust Model. Furthermore, this work aims to address the gap in the prevention of academic dishonesty in IHLs by outlining the components of academic integrity. As result, this study seeks to provide an in-depth examination of universities' policy on academic integrity, identify cultural and technological shifts to academic integrity education policy, address faculty and student engagement in academic integrity initiatives, and identify priorities in preventing academic misconduct and promoting academic integrity. The main objective will be to develop a Zero Trust Model based framework for prevention of academic dishonesty.

1. Background Work

The Covid-19 pandemic has ushered in a new era in the academic world. An era characterized by remote teaching and learning. Traditional teaching and learning methods requires and allows for face to face interaction as well as human centric monitoring methods. The assessment of students especially for examination based and continuous based methods are under attack from unprecedented levels of dishonesty. All necessitated by the inability of the institutions of learning to have physical monitoring of the academic processes. This calls for a shift in methods of either examining or monitoring the students or both.

A larger attack region in institutions of higher learning has been opened by new teaching and learning initiatives and processes [1]. Apart from the conventional institutional based regulations, teaching and learning software and platforms, and technologies, there are credible threats to dissolving what was once the trustworthy boundaries. Institutions' protection and networks protection must expand in order to safeguard business of learning institutions especially examinations and assessments for candidates[1].

It is a basic necessity for all educational institutes that students and staff have secured access to teaching and learning software installed behind the firewall. Educational institutes must also deal with the riskier proposition of providing access to a varied list of contractors, suppliers, partners, customers (students and staff), and developers[4].

Regardless of where these applications are hosted either in a public cloud or private data centers managing non face to face teaching and assessment is a complex, cumbersome task requiring a host of rules, regulations, hardware and software such as application delivery controllers (ADC) [4], virtual private networks (VPN)[5], identity and access management (IAM) systems, and more [5].

Yet with all of these technologies, educational institutions are still exposed to a variety of security risks stemming from the fact that access to internal applications opens up the entire network to attack[6] and there has never been a defined set of regulation to monitor control and regulate assessment and teaching methods online [7].

2. Zero Trust Security Architecture

Zero Trust Security is an IT security paradigm that involves stringent identity screening of any user and computer attempting to access services inside or outside the network perimeter[8], [9]. It is a systematic approach to network security that integrates many various concepts and innovations such that no single technology is related to zero trust [8].

Zero Trust was created by John Kindervag[10] to recognize that conventional security frameworks are built on the obsolete premise that everything in one organization's network should be trusted[10].

Installation of the Zero Confidence Model takes the form of an invalidation instead of assuming that anything behind the corporate firewall is secure[11]. Wherever the application originates, Zero Trust tells us "never believe, always check." Whatever the resource that the application uses [11].

Assuming that any user, request and server is not trusted until it has proved itself, every time a user or system requests access to a resource the zero-trust approach constantly and continuously tests its trust[11]. This strategy prevents attackers from exploiting weaknesses in the perimeter to gain entry, and, once inside, move laterally to access confidential applications and data[11].

The basis of Zero Confidence is the authentication of records[12]. Users, endpoints, applications and cloud services have become sources of communication that act as vectors of attack[12]. In a Zero Trust model in which nobody or any system can trust, it is the safest security strategy to concentrate the perimeter around data protection with intelligent authentication. Therefore, before Zero Trust begins to be enforced, agencies must clearly recognize their roles, responsibilities, data and technical properties [12].

Zero Trust does not depend on location[10]. Users, system and application workload are now all over, so Zero Trust must proliferate in the entire environment. One cannot apply Zero Trust in one place. The right users have to use the right applications and data.

Besides user access controls, zero trust often includes stringent system access controls [8]. Zero trust systems must track how many different devices attempt to access the network to ensure that all devices are authorised. This further minimizes the attack surface of the network[8].

A Zero Confidence replaces a perimeter-centric security [12] architecture. It guarantees the complex execution of protection and access decisions on the basis of identity, device and user context[12]. A security framework of the Zero Trust also specifies that application and data can only be accessed by authenticated and authorized users and devices. Simultaneously it protects certain applications and users against advanced Internet threats and attacks[12].

Cloud-based zero trust strategies represent a new security paradigm specifically designed to secure applications in the cloud and in your data center[8]. These solutions assume that there is no perimeter and that the environment is hostile and aggressive [8].

This Cloud based Zero Trust Architecture offers end users Single Sign-On (SSO) [8] capability for both their on-site and cloud based application systems. This is a control and authentication point. The end user sees all as the same. Cloud-based institutions now provide reliable, efficient, effective and productive security with their cloud-based solutions [8].

At the same time, it encourages IT to give any user access to specific applications, data and records, since a zero trust environment meets the least access principles. Safety administrators are no longer reluctant to give users (students and staff) access because they can be customized and carefully watched[11].

Zero Trust delivers both security and an excellent end-user experience. In the past, institutions have had to make trade-offs between strong security and a good, productive user experience.

Zero trust solutions offer secure access, productivity, and ease of use. Simple, convenient Multi-Factor Authentication (MFA) provides stronger security without the need to recall extreme passwords[10], [13]. SSO (single sign-on) further enhances the user experience and improves employee productivity by allowing users to log in to all of the applications which they require and have access to, without needing to authenticate each time or getting side tracked by syncing issues [10], [13].

Continuously adapting institutions' approach to security in response to evolving teaching and learning environments as well as threat landscapes is vital. Adapting a Zero Trust security architecture enables simple and effective safeguard of applications, users, and devices.

This paper proposes a Zero Trust Model with seven elements as tabled in Table 1 below. The proposed seven key elements of Zero Trust Architecture are zero trust networks, zero trust people, zero trust devices, zero trust workloads, zero trust data, validity and analysis, and automation and orchestration.

Table 1. Seven elements of the proposed HLI Zero Trust Model

No.	Key Element	Attributes/Description
1	Zero Trust Networks	• Ability to divide and rule the network to reduce lateral movement risk • Next Generation Firewall Implementations
2	Zero Trust People	• 81% of data breaches involving stolen credentials • Check Point Identity Awareness, email security, Multifactor Authentication, Context Aware Policies
3	Zero Trust	• Security teams must be able

	Devices	to isolate, secure, and control every device on the network at all times • Mobile Security, Advanced Endpoint Protection and Threat Prevention, IOT Security
4	Zero Trust Workloads	• Securing workloads are vulnerable, and attractive target to malicious actors • Cloud Security Management, Public Cloud Security
5	Zero Trust Data	• Protection of the data while it is shared continuously between workstations, mobile devices, application servers, databases, SaaS applications, and across networks • Data encryption, Data Loss Prevention, Data Management Categorization and Classification
6	Visibility and Analytics	• Constant monitoring of Logs, correlates, and analysis of every activity across the network. • Centralized Security Management, Security Event Management, Security Compliance
7	Automation and Orchestration	• Support of automated integration with the organization's broader IT environment to enable speed and agility, improved incident response, policy accuracy, and task delegations.

The seven elements are illustrated in Figure 1 where networks, data, devices, workloads and people form the outer vulnerable layer of the structure. These are the visible untrusted attack surfaces which needs to be treated with zero trust. Their specific activities are highlighted in Table 1. Automation and orchestration as well as visibility and analytics are also untrusted services provided by the machine based decision makers of the HLI systems. This covers all the activities which are at the centre of the model, the Education System.

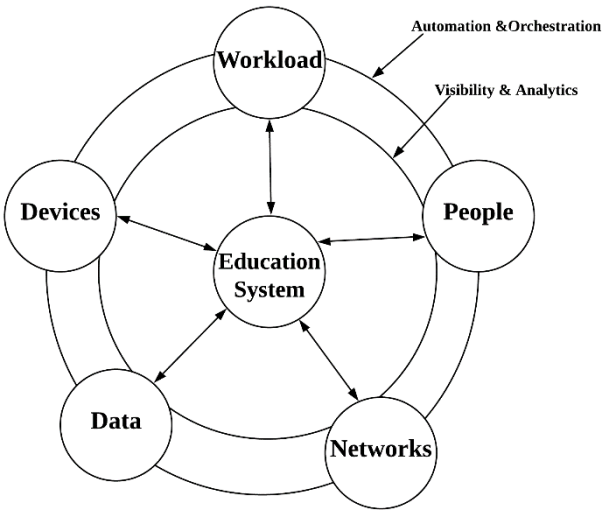

Figure 1. Proposed HLI Zero Trust Elements.

3. Existing countermeasures of academic dishonesty

Academic dishonesty refers to any actions undertaken to create an unfair academic gain, actions include plagiarism, cheating, giving/receiving aid on assignments, tests, and exams, and falsification of documents[14].

Academic dishonesty has undermined the integrity of our education systems demeaning the value of university education. This has led to academic institutions raising the alarm and putting in place ways and policies to prevent this behaviour. To begin with, some instructors have developed several versions of an exam instead of using a single exam more than one. This is because if the same exam is used over and over again, students will provide answers for others to see. Others have employed the use of plagiarism identification services to identify and prevent cheating. According to [15], some institutions have banned the use of electronic devices such as mobile phones, laptops, and PDAs during class and exams to prevent students from recording test information and sharing it with their friends. Students cheat when closely seated during exams. Invigilators get the students to sit further apart and even randomly assign seats during tests to prevent them from cheating.

Academic dishonesty has been deemed to create unfair advantage leading to the unfair competition when it comes to applying for scholarships, internships, and job offers. Therefore, it is the responsibility of academic administrators to ensure students are aware of the consequences of academic dishonesty and zero-tolerance policies to achieve academic integrity.

4. Components of academic integrity

Academic integrity is about the intellectual ethics of academic prosperity. This means one should be honest and responsible in pursuit of academic excellence. To achieve academic integrity, individuals are supposed to complete exams and assignments honestly, present accurate and truthful research data in academic projects, and avoid any act of plagiarism by incorporating and acknowledging cited sources accordingly. Academic integrity enhances exchange of ideas while working with and trusting one another[16].

Scholars, teachers, and administrators have the responsibility of embracing academic integrity because they comprehend the fruits of learning, teaching, and researching in an environment where ethical ideologies are upheld. This makes academic integrity a multi-dimensional aspect that is enhanced by all those in the educational institutions. Academic integrity is defined by six fundamental components: fairness, honesty, respect, responsibility, trust and courage (Fundamental values of academic integrity, 1999)

Table 2: Six fundamental components of academic integrity

No	Component	Details
1	Fairness	Every individual deserves fair treatment and be judged fairly by the same standards as others.
2	Honesty	Academicians thrive for truth and knowledge through sincerity. Every individual should acknowledge each other's ability and be able to represent their effort fairly.
3	Respect	Scholars appreciate the interactive nature of scholarship. In so doing, they value, honor, and contemplate diverse opinions and ideas of other scholars.
4	Responsibility	Academic societies of honesty rest upon pillars of personal responsibility combined with the commitment of individuals and organizations to lead by example, follow collectively agreed-upon values, and take action when they experience misconduct.
5	Trust	Facilitates working ties with other people and in the culture. Trust is built in a community in which all members do their best, in which processes and policies are equal and everyone is done equally.
6	Courage	Courage is an element of character that allows learners to commit to the quality of their education by holding themselves and their fellow learners to the highest standards of

		academic integrity even when doing so involves risk of negative consequences or reprisal.

Adhering to these six values is the true face of adversity. Without them, all efforts by scholars could become obsolete. If the core principles are accepted, used, and applied, they become a touchstone for the dignity of academic communities.

5. University policies on academic dishonesty

Academic dishonesty occurs when a member of an educational institution does not observe and maintain the values and principles of academic integrity. Learning institutions condemn academic dishonesty behaviour because it weakens the institution's values, quality of learning, and graduate results. Besides, academic dishonesty leads to the absence of trust in administrators, students, and faculties. For universities to uphold the highest standards of academic integrity across their community, policies have been implemented to support academic integrity across all learning, teaching, and researching activities (Code of Academic Integrity, 2019)

Students are responsible to produce their original academic work in any manner of presentation. Any assistance on academic work to be graded is prohibited unless approved by the instructor. Academic work presented for grading should include or sources cited. When assistance is offered completion of academic work, students are advised to acknowledge the contributor. If cited sources and acknowledgments are not present alongside the work submitted, it will be regarded as an act of dishonesty and disciplinary action will be administered (Code of Academic Integrity, 2019)

Instructors have been mandated to inform students about their expectations with regards to assistance, collaboration, acknowledgment, and citation of sources in each academic work. Students also have the responsibility of understanding and adhering to the principles that are relevant to academic work. In the event they do not understand the core principles, they should seek clarification and additional information (Carnegie Mellon University).

To summarize, these policies are implemented to support academic integrity. In return, academic transparency and competence are encouraged by the majority of the university systems. There is no room for any sort of academic dishonesty. According to a report by Burges, most university systems do not entertain dishonest attempts. Students convicted of university dishonesty can expect disciplinary action. Although the systems are designed not to tolerate academic dishonesty, the trends of academic have always been on an upward trend in HLI from 1960s with about 65% of the university students confirming they have cheated at least once in their academic journey. Most recently reports say more 95% of the students confessed to academic dishonesty activities, a worrying statistic. All this confirms failure of the existing methods towards stopping academic dishonesty. The main complication being caused by cultural and technological shifts in academic integrity towards ways and means to facilitate learning and student evaluations.

6. Cultural and technological shifts in academic integrity

Learning is an international affair. The number of international students in higher education is rapidly increasing [17]. Policies in the host country differ from those in the home country. Therefore, students' understanding of principles of academic integrity differs. Digital disruption has brought changes in the field of academics. Nowadays students make use of digital devices to undertake their studies. Most higher learning institutions are offering distance learning. All these advancements have led to convenient and improved efficiency in the education systems.

International students often tend to have little knowledge of the vices and principles of academic integrity in the host country. They, therefore, tend to lag when addressing the integrity principles of the institutions they are attending. This may raise alarm on the same. Therefore, it is the responsibility of stakeholders to ensure they are enlightened about the dishonesty behavior and its consequences. Teaching students about academic integrity differs in universities throughout the world. Therefore, universities have resorted to publishing their academic honesty principles as well as to engage their students in seminars and workshops to have a better understanding of the moral code of academia.

New technologies have impacted higher education by providing a platform for students to practice dishonest activities [18]. For instance, portable devices have facilitated discrete communication among students during exams to exchange answers. These devices are also capable of storing and accessing unauthorized material during exams. Luckily, instructors can also make use of technology to detect and prevent plagiarism as well as other academic irregularities.

This paper proposes a Zero Trust Architecture to disable human based trust and implement machine/algorithm (AI) based trust enforcement in a bid to restore integrity within the education system. The trust model is based on Core components, Supporting elements, and device and network infrastructure components. As defined in table 3.

Table 3: Zero Trust Model Components

Component	Sub Components	Description
Core components	policy engine	responsible for the ultimate decision to grant access to a resource for a given user/device. Confidence levels and ultimate access decisions are calculated by the policy engine
	policy administrator	responsible for establishing and maintaining the connection between a user/device and a resource
	policy enforcement	responsible for enabling, monitoring, and eventually terminating connections between a user/device and an enterprise resource.
Supporting elements	Continuous diagnostics and mitigation (CDM) System	gathers information about the current state of enterprise assets and applies updates to configuration settings and software
	Higher Education Compliance	includes all the policy rules that an enterprise develops to ensure compliance with any regulatory regime it may fall under
	Threat Intelligence	feeds funnel information collected from internal and/or external sources about newly discovered attacks or vulnerabilities to the policy engine to help make access decisions
	Activity Logs	responsible for recording traffic metadata seen on the network and for access requests made to enterprise resources
	Data access Policy	attributes, rules, and policies about access to enterprise resources. This set of rules could be encoded in or dynamically generated by the policy engine
	Public Key Infrastructure	responsible for generating and logging keys and/or certificates issued by the enterprise to resources, devices, and applications
	Identity Management	responsible for creating, storing, and managing enterprise user accounts and identity records
	Security information	collects security-centric information for later analysis.

	and event management (SIEM) system	This information is used to refine policies and warn of possible attacks against enterprise resources
Device and network infrastructure components.	Devices	include laptops, tablets, and other mobile or IoT devices that connect to the enterprise
	Infrastructure components	encompass network resources that a medium or large enterprise typically deploys in its environment. Zero trust architecture core and supporting components and devices are connected via the network infrastructure

The aim of this proposal is to provide a reference design and implementation that meets the following requirements:

- denotes a standards-based solution architecture that is an efficient and reliable method of applying a Zero Trust Architecture.
- allows easy access to the internet and business services, both on-premises and in the cloud, without the use of third-party software (e.g., virtual private network, trusted internet connection)
- demonstrates connectivity of cloud and on-premises business services
- illustrates integration of common directory protocols and identity management systems (e.g., Lightweight Directory Access Protocol [LDAP], Active Directory, OpenLDAP, Security Assertion Markup Language)
- demonstrates desired corporate user interface protection specifications, such as:

i. Ensuring data security at rest protecting system vulnerabilities that might result in unauthorized access to data saved on or used by the device and device misuse

ii. Mitigating ransomware execution on the computer, which may lead to unwanted access to data stored on or accessed by the device, as well as device misuse.

iii. Reducing the possibility of data loss due to unintended, intentional, or malicious deletion or subterfuge of data stored on the computer

iv. Maintaining knowledge of and reacting to unusual or harmful activity inside and against the system in order to deter or diagnose a device breach, and remediating as soon as possible.

The proposed Zero Trust Architecture for Institutes of Higher Learning is summarised in Figure 2 below.

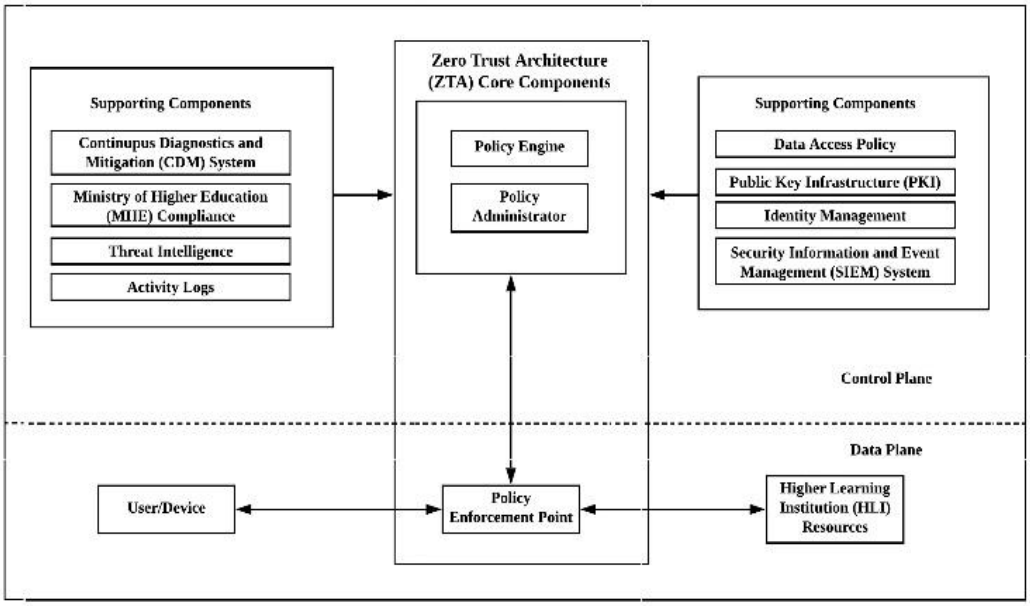

Figure 2: Zero Trust Architecture for Institutes of Higher Learning

In conclusion, new technologies and social norms [19] are changing the academic environment challenging the insights of academic integrity. Therefore, students' understanding of these policies differs from those of the instructors. HLI stakeholders are encouraged to update their policies dealing with the impacts of culture and technology on academic dishonesty and the Zero Trust Architecture is seen here as the way forward..

References

1. Chirumamilla, G. Sindre, and A. Nguyen-duc, "Assessment & Evaluation in Higher Education Cheating in e-exams and paper exams : the perceptions of engineering students and teachers in Norway," Assess. Eval. High. Educ., vol. 0, no. 0, pp. 1–18, 2020.
2. J. R. Elisha Tadiwa Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Abudhahir Buhari, Fares Anwar Hasan, "Prevalence of Premeditated Academic Dishonesty at University Level . A Case Study," J. Crit. Rev., vol. 7, no. 15, pp. 4494–4501, 2020.
3. P. J. PT Hogan, "Academic Dishonesty: A Study of CIS Student Cheating Behavior," J. Inf. Syst. Educ., 2020.
4. Ives and L. Giukin, "Patterns and Predictors of Academic Dishonesty in Moldovan University Students," 2019.
5. M. W. A. Abdul Wahab Muzaffar, Muhammad Tahira and S. R. M. Qaiser Chaudryb, "A Systematic Review of Online Exams Solutions in E-learning: Techniques, Tools and Global Adoption."
6. R. B. Moralista and R. M. F. Oducado, "Faculty Perception toward Online Education in a State College in the Philippines during the Coronavirus Disease 19 (COVID-19) Pandemic," vol. 8, no. 10, pp. 4736–4742, 2020.
7. Chen, J. Long, J. Liu, Z. Wang, and L. Wang, "Online Academic Dishonesty of College Students : A Review," vol. 448, pp. 156–161, 2020.
8. Decusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication," 2016.
9. B. Chen et al., "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," no. October 2018, pp. 1–16, 2020.
10. P. Assunção, "A Zero Trust Approach to Network Security," Digit. Priv. Secur. Conf., pp. 65–72, 2019.
11. T. Chuan, Y. Lv, Z. Qi, L. Xie, and W. Guo, "An Implementation Method of Zero-trust Architecture An Implementation Method of Zero-trust Architecture," 2020.
12. S. Dhar and I. Bose, "Securing IoT Devices Using Zero Trust and Blockchain Securing IoT Devices Using Zero Trust and Blockchain," J. Organ. Comput. Electron. Commer., vol. 00, no. 00, pp. 1–17, 2020.
13. C. De Weever and M. Andreou, "Zero Trust Network Security Model in containerized environments," pp. 1–12, 2020.
14. S. K. Hodges, "Academic Dishonesty in Higher Education : Perceptions and Opinions of Undergraduates," 2017.
15. S. Etter and J. J. Cramer, "Journal of Research on Technology in Education Origins of Academic Dishonesty," no. March 2015, pp. 37–41.
16. M. Green, J. East, and U. Mcgowan, "Core elements of exemplary academic integrity policy in Australian higher education," no. December 2014, 2011.
17. C. L. Chicago, "Succeeding as an international student in the United States and Canada .," p. 48479, 2008.
    A. L. Christensen, J. Cote, and C. K. Latham, UNAUTHORIZED ELECTRONIC ACCESS: STUDENTS' ETHICS, ATTITUDES, AND ACTIONS, vol. 11. Elsevier, 2015.
18. R. A. Bernardi, C. A. Banzhoff, A. M. Martino, and K. J. Savasta, "Accounting Education : An International Challenges to Academic Integrity : Identifying the Factors Associated With the Cheating Chain," no. January 2015, pp. 37–41.
19. Academic Dishonesty. (n.d.). Retrieved from https://www.montclair.edu/policies/all-policies/academic-dishonesty/
20. Academic Integrity Policy - Academic Integrity. (n.d.). Retrieved from https://www.uis.edu/academicintegrity/policy/
21. Burges, M. (n.d.). Academic Dishonesty. Retrieved from https://www.apus.edu/student-handbook/university-policies-and-honor-code/academic-dishonesty.html
22. Code of Academic Integrity. (2019). Retrieved from https://deanofstudents.arizona.edu/policies/code-academic-integrity

23. Five Pillars of Academic Integrity. (2014). Retrieved January 19, 2021, from https://www.unl.edu/gradstudies/connections/five-pillars-academic-integrity
24. Fundamental Values of Academic Integrity. (n.d.). Retrieved from https://www.palmer.edu/about-us/office-of-compliance/student-code-of-ethics/fundamental-values-of-academic-integrity/
25. Fundamental values of academic integrity. (1999). Durham, NC: Center for Academic Integrity, Duke University. How to Avoid Academic Dishonesty: Academic Integrity. (n.d.). Retrieved from https://www.luther.edu/academic-integrity/academicdishonesty/
26. McBurney, D. (1996). Cheating: Preventing and Dealing with Academic Dishonesty. Retrieved January 19, 2021, from https://www.psychologicalscience.org/observer/cheating-preventing-and-dealing-with-academic-dishonesty
27. McCabe, D.L., Butterfield K. D., & Trevino, L. K. (2006). Academic Dishonesty in Graduate Business Programs: Prevalence, Causes, and Proposed Action. Academy of Management Learning & Education, 5(3). Retrieved January 19, 2021, from https://doi.org/10.5465/amle.2006.22697018
28. Pincus, H., & Schmelkin, L. (2003). Faculty Perceptions of Academic Dishonesty: A Multidimensional Scaling Analysis. The Journal of Higher Education, 74(2), 196-209. Retrieved January 19, 2021, from http://www.jstor.org/stable/3648255
29. Sayed, N., & Lento, C. (2015). The impact of technology on academic dishonesty: Perspectives from accounting faculty. Available at SSRN 2655615.
30. Thompson, L. W., Bagby, J. H., Sulak, T. N., Sheets, J., & Trepinski, T. I. (2017). TheCultural Elements of Academic Honesty. Journal of International Students, 7(1), 136-153. University, C. M. (n.d.). Academic Integrity - University Policies - Carnegie Mellon University. Retrieved from https://www.cmu.edu/policies/student-and-student-life/academic-integrity.html
31. University, C. (n.d.). Student Academic Dishonesty Policy. Retrieved from https://policies.catholic.edu/students/academicundergrad/integrityfull.html.