BGSU®
BOWLING GREEN STATE UNIVERSITY
Office of General Counsel

VIA UPS OVERNIGHT MAIL
May 25, 2017

OFFICE OF INSPECTOR GENERAL
2017 MAY 26 AM 10: 02

Randall J. Meyer, Inspector General
Office of the Inspector General
30 East Broad Street, Suite 2940
Columbus, OH 43215

Re: *Bowling Green State University's Response to Report of Investigation Ohio File ID No. 2015-CA00048*

Dear Mr. Meyer:

INTRODUCTION

On March 28, 2017, the Office of Inspector General ("OIG") issued a Report of Investigation concerning Bowling Green State University Associate Dean/Professor Alan Atalah. In addition to setting out the OIG's findings and conclusions, the Report at page eleven directed the BGSU Provost to:

1. Review the actions of Alan Atalah, Ph.D., to consider whether administrative action is warranted.

2. Conduct a review of the current university internet usage policy with the goal of having a structure similar to the policy of the Ohio Department of Administrative Services for State of Ohio government agencies.

This is the University's Response to those directions.

UNIVERSITY'S REVIEW OF ALAN ATALAH'S ACTIONS

After inquiring into this matter, the University adopts the OIG's findings as its own.

The University directed Atalah to provide a response to the OIG's report. Through his private attorney, Atalah provided the response that is **Attachment A** to this Response. In summary, Atalah's explanation is: (1) He did not use a University computer to access the non-work related and inappropriate Conversations.doc file on the internet; (2) He intended to download the Conversations.doc file only to his own personal computer; (3) When downloading the file to his personal computer, Atalah inadvertently copied the document to the ODOT project file he had

308 McFall Center
Bowling Green, OH 43403
www.bgsu.edu
gencounsel@bgsu.edu
419.372.0464
419.372.8700 (F)

open on his personal computer at the time; and (4) He then unknowingly and inadvertently copied the Conversations.doc file now contained in the ODOT project file to the flash drive that was eventually delivered to ODOT.

The University finds that Atalah's explanation does not refute the OIG's material findings, nor does it mitigate his violation of the University acceptable use policy (BGSU Information Technology Policy 3341-6-7; **Attachment B**) or his failure to meet the University's expectations of professionalism.

ADMINISTRATIVE ACTIONS

The Report indicates that federal law enforcement found no grounds for criminal prosecution under federal law. The Wood County prosecutor reached the same conclusion concerning violations of state law (**Attachment C**).

The University finds that Atalah's actions violated the University's Information Technology Policy 3341-6-7 and were inconsistent with the professionalism BGSU expects of its academic administrators. His conduct warrants administrative action.

At all times relevant to these matters Atalah was appointed as an Associate Dean in the College of Technology, Architecture, and Applied Engineering (formerly the College of Technology). An Associate Dean is an academic administrator who serves at the pleasure of the college Dean and, by extension, University Provost. Academic administrators like Atalah are most often faculty who hold a tenured faculty appointment and so they have the right to return to their tenured position when the administrative appointment ends.

Atalah has no history of prior discipline, either as an administrator or as a member of the faculty.

The University is taking the following actions in connection with Atalah's employment:

1. Terminated as Associate Dean effective immediately.
2. Suspended without pay until the beginning of the Fall 2017 semester when he shall return to his tenured faculty appointment at his faculty salary.
3. A written reprimand will be placed in his personnel file.
4. Evaluations for 2016 shall be "does not meet expectations."
5. Ineligible to apply for externally funded grants for a period of two years but must focus on professional and personal improvement.
6. As directed by BGSU Information Technology Services, Atalah shall attend training on ITS policies regarding use of University technology resources.
7. Atalah will attend appropriate assessment with a licensed professional to address any issues related to the conduct involved in this matter. Atalah shall verify his attendance at assessment and, if indicated, counseling.
8. Atalah's use of University technology resources shall be subject to regular and unannounced compliance monitoring.

9. Any further serious violation of University policies by Atalah will result in immediate termination.

REVIEW OF THE CURRENT UNIVERSITY INTERNET POLICY

BGSU has reviewed the ODAS Internet Use Policy (IT-04) as requested in the Report.

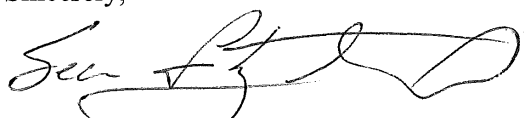
BGSU Information Technology Policy 3341-6-7 permits employees to use University IT resources for "limited social purposes." As it relates to an employee's permissible personal use of IT resources, the ODAS policy differs from the current BGSU policy in that it modifies the phrase "limited personal use" by adding the word "strictly". The ODAS policy also specifically lists a number of unacceptable personal uses, including the downloading or storage of "sexually explicit material."

The drafters of the BGSU Acceptable Use of Information Technology Policy were mindful of the importance of balancing the University's mission of researching, creating and disseminating knowledge with the need to appropriately constrain its employees' personal use of University IT resources. The internet is an important academic research tool and the University believes its current policy adequately strikes that balance.

That noted, BGSU will direct the relevant University policy makers to consider the OAD Internet Use Policy and make recommendations about which parts of it may be appropriate for inclusion in the University IT policy. We expect that review to occur in the 2017-18 academic year.

Should you have any questions or concerns, please feel free to contact me.

Sincerely,



Sean P. FitzGerald
Vice President and General Counsel

cc: Mary Ellen Mazey, President
Rodney Rogers, Provost and Senior Vice President
William Balzer, Vice President for Faculty Affairs and Strategic Initiatives

MALONE, AULT & FARELL

Attorneys At Law
7654 W. BANCROFT STREET
TOLEDO, OHIO 43617-1604

Richard R. Malone
Tim A. Ault
Gregory C. Farell
Bradley R. Waugh*
Milton E. Pommeranz*

Telephone 419 843-1333
Fax 419 843-3888
Email belazis@maf-law.com

Paul T. Belazis, Of Counsel**

* also licensed to practice in Michigan
** also licensed to practice in New York

April 28, 2017

Via email to: sfitzge@bgsu.edu

Sean P. FitzGerald, Esq.
Vice President and General Counsel
Office of General Counsel
Bowling Green State University
232 McFall Center
Bowling Green, Ohio 43403

Dear Mr. FitzGerald:

As you know, I represent Professor Alan Atalah in connection with the issues that have recently arisen following the issuance of a report by the Office of the Inspector General of Ohio dated March 28, 2017. I am in receipt of your correspondence to Dr. Atalah dated April 14, 2017 requesting that he respond to the information contained in the Inspector General's Report. Thank you for extending the time to provide this response.

The Inspector General's report describes an interview with Dr. Atalah that was conducted six months after receiving a complaint from the Ohio Department of Transportation about erotic material contained on a thumb drive. The thumb drive was submitted by Dr. Atalah to ODOT in April 2015 for the purpose of transmitting results of a research project conducted on ODOT's behalf. Not only was the interview conducted more than six months after the complaint was received and a year after the thumb drive was submitted to ODOT but Dr. Atalah was given no advance notice of the purpose of the interview. Instead, he was confronted with allegations and asked to immediately reconstruct events that had occurred at least a year earlier. We would also point out that, while ODOT began its investigation in September 2015, it was inexplicably not completed and its report was not issued until March 2017, more than a year and a half after the allegations arose. Furthermore, much of the information alleged in the report, including

information about files alleged to contain erotic material, was not shared with Dr. Atalah until now. The Inspector General's office did not bring the additional information to his attention, ask for a response, or conduct a follow up interview. We believe the delays and other failures associated with the Inspector General's investigation are prejudicial to Dr. Atalah.

As I understand the conclusions of the Inspector General's report, one piece of erotic literature was found on the thumb drive delivered to ODOT, three additional pieces of erotic literature were subsequently found on a university lap top issued to Dr. Atalah, and two "potentially" erotic MP4 videos are believed to have been deleted from the same lap top, as well as some unspecified number of other erotic stories. Dr. Atalah's response is a follows.

First, Dr. Atalah's duties at the university were wide ranging. He often worked long hours on administrative and research related responsibilities, frequently from his home. In addition, he regularly used his personal laptop or home desktop for work related duties. Consequently, Dr. Atalah routinely backed up and copied files from his personal computers to his university issued laptop. He did so to be assured of preserving files and, particularly, having access to work related data, reports, and other related information from all of these electronic devices.

Second, with respect to the Conversation.doc file, to the best of Dr. Atalah's knowledge and belief, the file was originally copied onto his personal computer while he was working on the ODOT project at home from his personal computer. At the time, the ODOT project folder was still opened. As a consequence, when copying the Conversations file onto his personal computer, the file was inadvertently copied onto the ODOT project folder. Dr. Atalah, of course, was not aware of the error. Consequently, when the ODOT project folder was subsequently copied onto a thumb drive for the purpose of transmitting it to ODOT, the Conversations file was also copied as it was still imbedded in the project folder.

Prior to copying the Conversations file, Dr. Atalah had not read it and was unaware of its content, other than that it was of an erotic nature. This was not unusual as he acknowledged to the investigator from the Inspector General's office, to whom he reported that he would sometimes cut and paste literature that he deemed erotic for later review. In the course of the interview with Dr. Atalah, the investigator revealed the name of the file (Conversations.doc."). Following the interview, Dr. Atalah was able to conduct a search and located the file, still embedded in the ODOT project folder on his personal computer as well as the version that had been subsequently downloaded as part of a routine backup onto his university laptop.

In short, the inclusion of this Conversations file document onto the thumb drive containing the project information was inadvertent. More important, it was not accessed using university technology. Instead, it was inadvertently copied onto the ODOT project file that was on a personal electronic device and subsequently inadvertently downloaded onto the university laptop as part of a backup conducted by Dr. Atalah for the purpose of ensuring preservation of and access to his work related information.

The Inspector General's report also references other documents containing erotic literature as well as evidence of deleted "potentially sexually explicit" videos that were alleged to have been discovered on Dr. Atalah's university lap top. Dr. Atalah was not made aware of these

allegations until receiving the report and the Inspector General's report does not provide sufficient information to directly address these allegations. In the absence of more information, these allegations are denied.

Finally, the Inspector General's report suggests that Dr. Atalah forwarded emails containing erotic literature from his personal email account to his university email account. These allegations are entirely inaccurate. There was no routine forwarding of emails of any kind from his personal email to his work email, as was suggested by the Inspector General's report. Nor was it necessary as Dr. Atalah was able to access all of his emails at any time, both personal and university related, without the need to forward.

I hope this response is helpful.

Sincerely yours,

Paul T. Belazis

Cc: William K. Balzar via email: wbalzer@bgsu.edu

BGSU®
BOWLING GREEN STATE UNIVERSITY

3341-6-7 BGSU Information Technology.

Applicability	All University units
Responsible Unit	The Vice President for Finance and Administration
Policy Administrator	The Office of the Chief Information Officer

(A) Policy Statement and Purpose

Bowling Green State University provides information technology resources to support the academic, administrative, educational, research and service missions of its appropriately affiliated members within the margins of institutional priorities and financial capabilities. The information technology resources provide for the university, a conduit for free and open forum for the expression of ideas mindful of the university core values. In order to protect the confidentiality, integrity, and availability of information technology resources for intended purposes, the following policy has been developed.

(B) Policy Scope

The scope of this policy is to encompass all information technology devices owned by the university, any device obtaining connectivity to the university network, and all university relevant data on these devices.

(C) Policy

(1) All usage of information technology resources is to be consistent with all other relevant policies at BGSU.

(2) Users must be aware of and comply with all Federal, State, local, and other applicable laws, contracts, regulations and licenses.

(a) US Code

(b) Ohio Revised Code

(c) Digital Millennium Copyright Act (DMCA)

(d) Electronic Communications Privacy Act (ECPA)

(e) Computer Fraud and Abuse Act (CFAA)

(f) Family Educational Rights and Privacy Act (FERPA)

(g) Health Insurance Portability and Accountability Act (HIPAA)

(h) Gramm-Leach-Bliley Act (GLBA)

(i) House Bill 104

(3) Use of information technology to access resources other than those supporting the academic, administrative, educational, research and service missions of the University or for more than limited social purposes is prohibited.

(a) Information technology is provided to access resources supporting the academic, administrative, education, research and service missions of the university. Use of the provided information technology resources is to be mindful of the university core values. Use of information technology for experimental use or limited social purposes is permitted, as long as it does not violate other policies or interfere with operations of the university.

(b) The legitimate use of information technology resources does not extend to whatever is technically possible. Although some limitations are built into computer operating system and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

(c) Network applications and protocols that are not essential to carrying out the mission of the university or to conduct university business are neither specifically permitted nor specifically prohibited. Should such a subsidiary application or protocol become a risk to the security of the university's information technology infrastructure, its use will be restricted or blocked as deemed appropriate or necessary, without prior notice.

(4) All users must only access or attempt to access information technology resources that they are authorized to use and then only in a manner and to the extent authorized.

(a) Ability to access information technology resources does not, by itself, imply authorization to do so. Prior to accessing a resource, users are responsible for ascertaining and properly obtaining necessary authorization. Accounts, passwords, and other authentication mechanisms, may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the university.

(5) Attempting to circumvent information technology security systems is prohibited.

(a) BGSU employs various technologies and procedures in the interest of protecting the confidentiality, availability, and integrity of information technology. Some examples of these technologies and procedures, include, but are not limited to, physical methods, firewalls, anti-virus software, encryption, and passwords. Circumvention or attempted circumvention of a security system creates a threat to the university and is not permitted.

(6) Disruption of university authorized activities is prohibited.

(a) All members of the BGSU community share the information technology resources provided by BGSU. Those causing disruption to the use of information technology resources for other community members will be

in violation of this policy. Some examples include, but are not limited to, configuration of devices that disrupt network services, launching denial of service attacks, and disturbing public access resources.

(7) Use of information technology to conduct reconnaissance, vulnerability assessments, or similar activity by unauthorized personnel is prohibited.

(a) In an effort to protect the confidentiality, availability, and integrity of information technology resources, BGSU officials will investigate any discovered unauthorized network reconnaissance, vulnerability scanning, or service enumerations. While it is recognized that there are some valid purposes for this activity, BGSU officials are unable to determine intent and must react in a manner that will best protect information technology resources by assuming that the source of scans are malicious. Additionally, many vulnerability scanning tools utilize techniques that may be disruptive if not properly used. Please contact the ITS Information Security Office for authorization to conduct vulnerability or service assessments using BGSU information technology resources.

(8) Users are required to protect the confidentiality, integrity, and availability of information technology.

(a) This responsibility includes practicing safe computing at all times when deploying or using BGSU information technology resources. Users are to care for the integrity of technology based information sources they are authorized to access and to ensure that information is shared only with other appropriately authorized users.

(9) Anonymous use, impersonation, or use of pseudonyms on an information technology resource to escape accountability is prohibited.

(a) Examples of this include, but are not limited to, forging email or using any Internet service not affiliated with the university that can prevent accountability for its usage.

(10) The use of any unlicensed spectrum space is prohibited on any BGSU-owned or BGSU-occupied property, unless it is part of the wireless services being deployed by the university.

(a) Information Technology Services (ITS) has implemented wireless Local Area Network (LAN) services on the BGSU main campus and the Firelands campus. While this service allows mobility and easier access to the BGSU network, it means that the air space on campus now serves as a medium for network connectivity. The use of open air space poses a number of potentially difficult situations for both users and network administrators. Users that may need to make use of wireless equipment for special purposes such as research or other unique applications must contact the Technology Support Center within ITS to coordinate this use of wireless air space.

(11) Responsibilities

(a) University Responsibilities

(i) Provide and coordinate information technology resources to allow completion of duties as assigned in support of the academic, administrative, educational, research, and service missions, within the margins of institutional priorities and financial capabilities.

(ii) Communicate, review, update, and enforce policies to protect information technology resources.

(iii) Take reasonable measures to mitigate security threats.

(b) User Responsibilities

(i) Read, agree to, and abide by all university policies and policy updates.

(ii) Practice safe computing when using information technology resources.

(iii) Notify university officials upon discovery that an assigned information technology resource has been accessed, attempted to be accessed, or is vulnerable to access by unauthorized users.

(iv) Users are responsible for activity resulting from their assigned information technology resources.

(12) Security and Privacy Statement

BGSU respects the privacy of all information technology users. The university does not routinely monitor the content of material but does reserve the right to access and review all aspects of its information technology infrastructure to investigate performance or system problems, search for harmful programs, or upon reasonable cause, to determine if a user is violating a policy, State or Federal law. BGSU monitors, keeps, and audits detailed records of information technology usage; traces may be recorded routinely for trouble shooting, performance monitoring, security purposes, auditing, recovery from system failure, etc.; or in response to a complaint, in order to protect the university's and others' equipment, software, and data from unauthorized use or tampering. Extraordinary record keeping, traces and special techniques may be used in response to technical problems or complaints, or for violation of law, policy or regulations, but only on approval by university administrators specifically authorized to give such approval. In addition to the privacy of individuals being respected under normal circumstances, the privacy of those involved in a complaint will be respected and the university will limit special record keeping in order doing so, where feasible. Information will be released in accordance with law. Users should be aware that while the university implements various security controls to protect information technology resources, protection of data from unauthorized individuals cannot be guaranteed.

(13) Enforcement and Sanctions

Individuals or entities in violation of the BGSU Information Technology Policy will be referred to the appropriate disciplinary authority for review. Access privileges may be suspended without prior notice if it is determined that a policy violation is causing a current or imminent threat to the confidentiality, integrity, or availability of information technology resources.

(14) Implementation of Policy

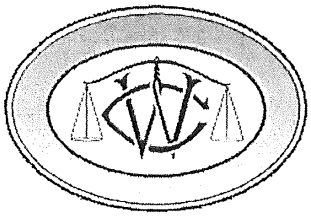
This policy replaces the Information Technology Services Network and Computer Policies and the Acceptable Use Policy for Information Technologies and is authorized by the Office of the Chief Information Officer (CIO) and has been approved by the appropriate university committee(s). This policy may be supplemented with additional published guidelines by campus units that are authorized to operate/control their own information technology resources provided such guidelines are consistent with and supplemental to this policy and do not alter its intent.

(15) Related Policies

(a) Codes of Student Conduct, BGSU Copyright Policy, Administrative Staff Handbook, Classified Staff Handbook, Intermittent Classified Staff, Retirees Handbook, Academic Charter

Registered Date: March 17, 2015
Amended Date: March 31, 2016

PAUL DOBSON



WOOD COUNTY
PROSECUTING ATTORNEY

CRIMINAL DIVISION
Thomas Matuszak, Chief
Aram Ohanian
David Romaker, Jr.
Alyssa Blackburn
J. Christopher Anderson
Channa Beard
David Harold, Appellate
Douglas Kinder, Investigator
Brynn Burr, Investigator
Michelle Mossbarger, Paralegal

VICTIM WITNESS
Monica DeLeon, Director
Katelin McGowan, Assistant

CIVIL DIVISION
Arlen de la Serna, Chief
Linda Holmes
Carri Stanley
Kimberly Edelstein

JUVENILE DIVISION
Charles Bergman, Chief
Walter Meneses
Heather Baker

C.Y.C.L.E. DIVISION
Brandy Hartman, Director
Sydney Pryka, Assistant

MAILING ADDRESS
One Courthouse Square
Office Building, 4th Floor
Bowling Green, Ohio 43402

PHONE
419.354.9250

FAX
Criminal 419.353.2904
Civil & Juvenile 419.354.7627

WEBSITE
woodcountyprosecutor.org

Writer's e-mail
pdobson@co.wood.oh.us

OIG File 2015-CA00048
BGSU ATTACHMENT C

April 5, 2017

Randall Meyer
State of Ohio Inspector General
Rhodes Stare Office Tower
30 East Broad Street, Suite 2940
Columbus, Ohio 43215-3414

Re: Alan Atalah Investigation

Dear Mr. Meyer:

I have reviewed the relevant information provided me by your office on the above-captioned investigation. While I find the material offensive in the extreme, I am not confident that a prosecution of Mr. Atalah would result in a conviction. I am therefore declining prosecution of this matter.

Thank you for bringing this to my attention. Should you have any questions or concerns regarding this decision, please feel free to contact me.

Sincerely,

Paul A. Dobson
Wood County Prosecuting Attorney