Public Records Exemption for Security-Related Information

Effective: May 17, 2007

Updated/Revised: April 6, 2011

Contact: <u>Public Records Officer</u>

Introduction

Iowa law (Iowa Code §§ 22.7(50) and 22.8) allows non-disclosure of security-related information when the institution has a policy exempting such information or where the disclosure would not be in the public interest. Disclosure of certain information may increase risks to persons and facilities. This policy is intended to increase the safety and security of persons and property on the campus.

Policy Statement

The following information may be withheld in responding to public records requests in order to protect safety and security at the University:

1. Information about alarm and security systems used at the university including key codes, passwords, electronic codes, wiring diagrams, plans and security procedures and protocols related to such security systems.
2. Information about security systems governing access to information technology systems, including passwords, protocols and security hardware and software.
3. Security protocols and technical information related to the configuration, access to, design and location of key assets related to utilities, including the power plant, utility tunnels, water, electrical lines and information technology infrastructure.
4. Portions of architectural and engineering designs, and other technical information, which are not otherwise publicly available, and which, if disseminated, would significantly compromise the security of a University-owned or leased building or facility.
5. Security plans and protocols, including security-related contingency planning and emergency response plans.
6. Information related to location of individuals and groups may be withheld in the following situations:
    a. Travel plans, locations, schedules and itineraries for high-profile individuals visiting the campus;
    b. Travel plans, locations, schedules and itineraries of an individual or group when specific threats are known to exist for the individual or group;
    c. Travel plans, locations, schedules and itineraries of persons conducting specified activities when there is a known and reasonable risk of harm to persons conducting the activity; and
    d. Reserved seating locations and room numbers of individuals attending events or renting rooms for private purposes.

38 7.   Information about specific threats, assessment of specific threats and plans for addressing
39   specific threats held by university-recognized threat assessment teams.
40 8.   Information about the location of, and protocols used for sensitive research projects,
41   materials and subjects when there is a known and reasonable risk of sabotage or damage to
42   the project, the materials or subjects of the research.
43 9.   Information about the protocols, methods, facilities and equipment used in food production,
44   which is not publicly available, and which, if disseminated, would significantly compromise
45   the security of food production or preparation.
46 10.   Information about the location of hazardous materials such as controlled substances,
47   radioactive materials, toxic or reactive materials, ingredients for toxic or reactive materials,
48   explosives and hazardous biological materials.
49 11.   Security protocols and information related to cash, cash equivalents and property with
50   unique or extraordinary value.
51 12.   Assessments of security vulnerability of the campus or specific campus assets or systems.

52 The above exemptions are not intended to apply to any information which has been publicly
53 announced or is otherwise readily available. Only information that has a reasonable likelihood of
54 jeopardizing safety should be withheld under this policy. A person denied access to the above
55 information may appeal the decision to the university's Public Records Officer.

56 # Resources

57 **Links**

58 • Iowa Code 22.7(50)
59 • Iowa Code 22.8
60 • Guidelines on public records requests
61 • Exchange Email Best Practices