



1 **IT POLICY 103: VIRUS, TROJAN, SPYWARE and OTHER**
2 **MALICIOUS CODE PREVENTION**

3
4 ISSUED BY THE OFFICE OF INFORMATION TECHNOLOGY FOR INTERNAL USE.
5

6 **Policy Review Period: Semi-annually**

Security Response Priority Level: (TBD)

7 **TECHNICAL POLICY STATEMENT**

8 **TECHNICAL POLICY:** *All UNLV non-mainframe computers, network-connected or non-networked,*
9 *shall employ a strong anti-virus application. Additionally, it is strongly recommended that all UNLV*
10 *network-connected computers should employ an anti-spyware application. This policy establishes the*
11 *minimum standard which must be met by all small UNLV computers to ensure effective virus, malicious,*
12 *and other malware prevention or detection and removal.*

13
14 **OBJECTIVES:** To provide management direction and support for information security in accordance
15 with internationally accepted standards (ISO 17799/27001), business requirements and relevant State
16 and Federal laws and regulations. To support a robust, service-oriented, flexible Information
17 Technology Infrastructure to sustain continued pursuit of UNLV institutional goals. This technical
18 policy directly supports the capstone UNLV Global Information Security Policy. The network
19 infrastructure and other IT resources need to be continuously protected from threats posed by computer
20 viruses, worms, spyware, and other types of malicious or malware code. The protection of individual or
21 end-point systems contributes to the baseline security structure for a defense-in-depth integrated
22 security.

23
24 **SCOPE AND APPLICABILITY:** The Policy applies to all University computing systems. The
25 information technologies covered by the policy include all systems, networks, and facilities
26 administered by Office of Information Technology (OIT), as well as those administered by individual
27 schools, departments, University laboratories, and other University-based entities.

28
29 Use of UNLV networks, even when carried out on a privately owned computer that is not managed or
30 maintained by UNLV, is also governed by this Policy when the computer is connected to the network.

31
32 **BACKGROUND:** The virus, spyware, and other malware threats have the potential of causing
33 significant business and academic disruption and significant cost in terms of failed services, service
34 recovery, and costs associated with the potential loss of protected or sensitive information.

35
36 The purpose of this Policy is to:

- 37
38
 - Establish the mandatory use of anti-virus and malicious code applications.
 - Ensure that access to UNLV electronic resources are reasonably secure.

39
40
41 University of Nevada, Las Vegas has established specific guidelines, outlined in this document, for
42 implementation and legal compliance of processes to be used for the purpose of computer protection.

43 This policy does not apply to non-UNLV computing systems except when connected to UNLV
44 networks.

45
46 In order to manage information security comprehensively, this policy aims to promote the following
47 goals:

- 48
- 49 • To ensure that use of IT systems is consistent with sound security principles;
 - 50 • To ensure that IT systems are used for their intended purposes and meet any compliance
51 requirements;
 - 52 • To ensure the integrity, reliability, availability, and superior performance of IT systems;
 - 53 • To assure that the core IT network and systems is available to support emergency services in
54 the event of community disaster response needs; and
 - 55 • To establish standards for addressing security consistency.
- 56

57 **POLICY STANDARDS AND CONTROLS:** See the ANNEX below titled STANDARDS for
58 mandatory baseline Policy Standards and Controls that are required to be implemented to be in
59 minimum compliance with this policy and its objectives.

60

61 **COMPLIANCE:** It is the responsibility of the UNLV Provost's Office of Information Technology to
62 administer and maintain this Policy and all related information security policies. The Policy shall also
63 be maintained and enforced with assistance from the UNLV Provost, UNLV Administrative Code
64 Office and NSHE Counsel, and NSHE System Computing Services (SCS). Policy compliance
65 requirements are:

66

- 67 1. UNLV management has the responsibility to manage University information, personnel, and
68 physical property relevant to academic and business operations, as well as the right to monitor
69 the actual utilization, but not the content except under pre-approved conditions, of all
70 University assets.
 - 71 2. Information security reviews and security audits will be conducted annually or more frequently
72 as required. The OIT Information Security Officer (ISO), or appointed designee, will conduct
73 security policy reviews and security audits.
- 74

75 In addition to any possible legal sanctions, UNLV employees and students who fail to comply with the
76 policies will be considered in violation of the University's relevant codes of conduct and may be subject
77 to disciplinary action up to and including dismissal or expulsion, pursuant to Campus policies,
78 collective bargaining agreements, codes of conduct, or other instrument governing the individual's
79 relationship with the University. Recourse to such actions shall be as provided for under the provisions
80 of those instruments.

81

82 **AUDIT STANDARDS AND CONTROLS:** Compliance and effectiveness auditing of this policy shall
83 be accomplished using the appropriate BS 7799.2:200x Audit Check List, dated 8.08.2005 or later, and
84 through a complete review of all related misuse complaints (security incidents) that occurred after the
85 previous audit. The audit shall inspect the in-use security applications, procedures, and processes of
86 systems supporting this policy, including timeliness of updates, for compliance to the policy. The OIT
87 ISO, or designee, shall be the ombudsman, manager and principal reviewer of this policy. Proposed
88 adjustments and enhancements to the policy for unforeseen issues shall be presented to the designated
89 workgroup or committee for approval. An audit report and recommendations shall be sent to the Vice
90 Provost for Information Technology.

91
92 **ROLES AND RESPONSIBILITIES:** See the ANNEX for ROLES AND RESPONSIBILITIES for
93 the policy responsibilities of Administrative Officials, IT Providers, and Users.
94

95 **MONITORING, NON-COMPLIANCE AND EXCEPTIONS**

96
97 **MONITORING (VIOLATIONS):** It is an explicit violation of this policy to do any of the following:
98

- 99 1. Knowingly or intentionally attach mis-configured IT devices to the network.
- 100 2. Knowingly or intentionally compromise a network, system, or database.
- 101 3. Knowingly or intentionally, (or negligently after receiving notice from an information
102 technology officer or professional), transmit any computer virus or other form of malicious
103 software.
- 104 4. Knowingly or intentionally access or exploit resources for which you do not have authorization.
- 105 5. Knowingly or intentionally perform network or system scans on resources not authorized by the
106 IT Security Director, unit head, unit security liaison, or local support provider.
- 107 6. Knowingly or intentionally fail to implement the security policies and directives related to the
108 IT resources for which you control or administer.

109
110 **NON-COMPLIANCE (ENFORCEMENT):** Suspected policy violations will be investigated by the
111 OIT Information Security Officer and the appropriate office, and disciplinary actions may be taken in
112 accordance with the NSHE, UNLV Bylaws, and Student Code of Conduct applicable regulations, or
113 other University policy.
114

115 **Reporting Observed Violations.** If an individual has observed or otherwise is aware of a violation of
116 this Policy, he or she must report the violation to the OIT Information Security Office.
117

118 **Disciplinary Procedures.** Alleged violations of this Policy will be pursued in accordance with the
119 appropriate disciplinary procedures for faculty, staff, and students. The OIT Information Security
120 Officer will refer these cases for disciplinary action to the following officers:
121

- 122 • If the alleged violator is a student, the Student Conduct Officer.
- 123 • If the alleged violator is a classified staff employee, Human Resources.
- 124 • If the alleged violator is a professional staff employee, the Administrative Code Officer.

125
126 Systems administrators and the Information Security Office may participate in the disciplinary
127 proceedings as deemed appropriate by the relevant disciplinary authority.
128

129 **Legal Liability for Unlawful Use.** In addition to University discipline, Users may be subject to
130 criminal prosecution, civil liability, or both for unlawful use of any University IT system.
131

132 **EXCEPTIONS: (None)**
133

134 **CONTACTS**

135 OFFICE OF INFORMATION TECHNOLOGY

136 INFORMATION SECURITY OFFICE

137 Herman W Westfall (HWB), Room 101
138 (702) 895-3628 / FAX (702) 895-1847
139

140 **DEFINITIONS**

141 **Key Definitions for this policy: none.**

142

143 **Additional Definitions** of terms in this and other policies can be found in UNLV OIT document
144 "***Information Security Acronyms, Terms and Definitions***".

145

146 **ATTACHMENTS:** *Anti-Virus Guidelines*

147

148

148

149

ANNEX-1: POLICY STANDARDS

150

BASELINE SECURITY STANDARDS AND CONTROLS. The following are the Policy Standards that shall be implemented to be in minimum compliance with the Policy.

151

152

153

Personnel are required to read the NOTICES below. The POLICY STANDARDS in the following UNLV Policies shall be read for issues related to acceptable and unacceptable behavior requirements:

154

155

156

Acceptable Use of UNLV IT Resources (Users) Policy

157

Acceptable Use of UNLV IT Resources (Mgmt & SysAdmin) Policy

158

159

STUDENT RESPONSIBILITIES:

160

POLICY STANDARD: 103-1 Anti-Virus for Personal Computers. All personal-style (laptops & desktops) computers shall have UNLV's standard, supported anti-virus software, or approved alternate, installed and actively running when connected to UNLV networks. In addition, the anti-virus software and the virus signature/pattern files must be kept up-to-date. Virus-infected computers must be removed from the network or quarantined until they are verified as updated and virus-free. System administrators are responsible for creating and enforcing procedures that ensure anti-virus software is running on network connected computers, and the computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into UNLV's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy* and the *Acceptable Email Usage Policy*.

161

162

163

164

165

166

167

168

169

170

171

172

POLICY STANDARD: 103-2 Anti-Spyware for Personal Computers. All personal-style (laptops & desktops) computers are strongly recommended to have a UNLV recommended standard anti-spyware application, or approved alternate, installed and actively running when connected to UNLV networks. In addition, the anti-spyware software and the spyware pattern files should be kept up-to-date. Spyware-infected computers should be removed from the network or quarantined until they are verified as updated and clean. System administrators are granted permission to create and enforce anti-spyware procedures where needed and that the computers are verified as clean.

173

174

175

176

177

178

179

180

POLICY STANDARD: 103-3 Anti-Virus for Small Computing Devices.: Computer devices such as PDA's with operating systems that do not have commercial anti-virus software available for use are exempt from this policy until the software becomes available. Refer to UNLV's *Anti-Virus Guidelines* below to help prevent virus problems.

181

182

183

184

185

186

ACADEMIC AND GENERAL STAFF RESPONSIBILITIES:

187

POLICY STANDARD: 103-4 Anti-Virus for Business/Application Servers. All departmental servers and other departmental-style small computers shall have UNLV's standard, supported anti-virus software, or approved alternate, installed and actively running when connected to UNLV networks. In addition, the anti-virus software and the virus signature/pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. System administrators are responsible for

188

189

190

191

192

193 creating and enforcing procedures that ensure anti-virus software is running on network
194 connected computers, and the computers are verified as virus-free.

195
196 **POLICY STANDARD: 103-5 Anti-Virus for Email Servers.** All email servers and other
197 departmental-style small computers operating an email service shall have UNLV's standard,
198 supported anti-virus software, or approved alternate, installed and actively running when
199 connected to UNLV networks. In addition, the anti-virus software and the virus
200 signature/pattern files must be kept up-to-date. Virus-infected computers must be removed from
201 the network until they are verified as virus-free. System administrators are responsible for
202 creating and enforcing procedures that ensure anti-virus software is running on network
203 connected computers, and the computers are verified as virus-free.

204
205 **POLICY STANDARD: 103-6 Any Network Connected Business/Application Computer.**
206 Network connected departmental/small computers that do NOT have UNLV's standard,
207 supported anti-virus software, or approved alternate, installed and actively running when
208 connected to UNLV networks shall be quarantined or removed from the network until they are
209 updated and verified as virus-free before allowing further access.

210
211 **SUPPLEMENTAL *Directives, Procedures, Handbooks, and Guidelines*, if included, are located in**
212 **the last section or appendices of the document.**

213
214 **INCORPORATED OTHER STANDARDS AND DIRECTIVES OF THE POLICY:** In addition to
215 the core security requirements and standards above, related Directives may be written and incorporated
216 to amend the primary Policy to address, define and promote special IT security standards for unique
217 groups of constituencies or security devices to ensure a secure and reliable information technology
218 infrastructure.

219
220
221

221

222

ANNEX-2: ROLES AND RESPONSIBILITIES

223

ACCOUNTABILITY:

224

225

Obligations of the User

226

227

Any individual who uses an IT device and has a UNLV computer or network account (see the "Definitions" section of this document) is a User.

228

229

1. Understanding and complying with current policies, requirements, guidelines, procedures, and protocols concerning the university electronic networks, devices, software, and electronic mail (see the "Related Documents" section of this document).
2. Complying with guidelines and practices established by the local system provider and the local electronic mail provider.
3. Updating campus-wide security applications, including anti-virus software and operating system updates, in a timely fashion (contact Campus Computing Services if you need assistance).
4. Protecting the resources under his or her control by using appropriate passwords.
5. Contacting the local system and email provider whenever a questionable situation arises regarding the security of the service.
6. Reporting all electronic security incidents to the local support provider or contact Campus Computing Services immediately, as detailed in University policy.
7. Assisting in the performance of remediation steps in the event of a detected infection, or compromise.

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

◆ Note: If you cannot perform or do not understand any of the obligations assigned to Users, contact the Campus Computing Services help desk.

246

247

248

Obligations of Local System Providers

249

250

A local system provider is the organization with principal responsibility for the installation, configuration, security, and ongoing maintenance of an IT device(s) (e.g., system administrator, network administrator, etc.).

251

252

253

254

The local service provider is responsible to do the following:

255

1. Be knowledgeable and comply with the current policies, requirements, guidelines, procedures and protocols concerning the administration and security of the University information technology resources.
2. Maintain knowledge of IT devices under his or her control through identification and understanding of their usage.
3. Follow appropriate best practices guidelines and directives for configuring and maintaining IT systems and anti-virus applications.
4. Understand and document the specific configurations and characteristics of the IT devices he or she supports to be able to respond to emerging information technology threats and to support recovery and mitigation efforts appropriately.
5. Understand and recommend the appropriate measures to provide security to the resources under his or her control, including, but not limited to:

256

257

258

259

260

261

262

263

264

265

266

267

- 268 • full implementation of the most current authentication and authorization technologies
269 utilized by the architecture of the university network and/or its technology resources;
270 • the most recently tested and approved software patches available;
271 • the most contemporary and available security configurations;
272 • the most contemporary and available virus/malicious code protection.
273
274 6. Collect appropriate information regarding devices compromised by electronic security
275 incidents. Disconnect affected information technology devices from the network, where
276 appropriate.
277 7. Follow electronic security incident reporting requirements in accordance with University
278 Policy, Reporting Electronic Security Incidents. Notify security personnel of electronic security
279 incidents and any remedial action taken.
280

281 ◆ Note: Local support providers should be mindful of potential responsibilities they may also have as
282 custodians of administrative data transmitted or stored on IT devices under their control.
283

284 **Obligations of the Unit Information System Security Liaison (ISSL) Person(s)**
285

286 The unit security person(s)/liaison is the person whom the unit head designates as the primary contact
287 for the OIT Information Security Officer (ISO) and is responsible for performing unit or system IT
288 security. For further guidance or clarification, contact the OIT Information Security Officer.
289

290 The unit security person(s)/liaison is responsible to do the following:

- 291 1. Act as the unit point of contact with OIT Information Security Officer.
292 2. Implement a security program consistent with the requirements of this policy and related
293 policies consistent with university guidelines and practices and in keeping with the specific
294 information security needs of his or her unit.
295 3. Act as the security coordinator for the local support provider(s) within his or her unit (in units
296 where the unit security liaison is not the local support provider).
297 4. Take appropriate actions to eliminate problem sources of traffic from the UNLV network, up to
298 and including blocking the information technology device.
299 5. Participate and assist the ISO, or designated representative, in conducting authorized
300 investigations within their unit.
301 6. Initiate escalation procedures, such as notification of the OIT Information Security Officer, Unit
302 Head, the UNLV Campus Police, or the Student Judicial Affairs Office as necessary.
303 7. Implement unit procedures and protocols for the reporting of electronic security incidents in
304 accordance with University Policy, Reporting Electronic Security Incidents including:
305
306 a. Open and maintain problem reports for electronic security incidents.
307 b. Contact users of and/or local support providers for compromised devices.
308 c. Communicate to local support providers and users, any actions that need to be taken,
309 the reasons for them, the steps required to reestablish service, and any relevant
310 technical information about the incident.
311

312 ◆ Note: The Unit Security Liaison may want to take specific measures toward the protection of data
313 stored or transmitted on the IT devices under his or her management and/or be mindful of any potential
314 responsibilities as custodians of administrative data.
315

316 **Obligations of the Unit Head**

317

318 Unit heads or individuals with responsibility for administrative units have overall, local responsibility
319 for the security of information technology resources under their control. For further guidance, contact
320 your Unit Security Person(s)/Liaison or the OIT Information Security Officer.

321

322 The unit head's oversight responsibilities in relation to security information technology resources
323 include, but are not limited to, the following:

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

◆ *Note: Unit heads may want to take specific measures toward the protection of data stored or transmitted on the IT devices under their management. Please consult with University policies on data stewardship and custodianship, for further guidance.*

344

Obligations of the UNLV Information Security Officer

345

346

347

348

The OIT Information Security Officer is the individual with the authority to coordinate campus information technology security and related investigations.

349

The obligations of the ISO are to:

350

351

352

353

354

355

356

357

358

359

360

361

362

1. Oversee, assist or lead electronic or security incident investigation and resolution for the University and individual units. Use approved computer forensic methodologies as required.
2. Ensure proper identification, analysis, resolution, and reporting of UNLV digital security incidents.
3. Oversee and support authorized university-level electronic monitoring and analysis.
4. Support and verify electronic communication privacy and security compliance with federal, state, and local legislation.
5. Develop a comprehensive security program that includes policies, risk assessments, best practices, education, and training.
6. Conduct/oversee IT security audits.

362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390

APPENDIX 1

ANTI-VIRUS GUIDELINES

General Prevention Guidelines

Recommended processes to prevent virus problems:

1. Always run the UNLV standard, supported anti-virus software available from the University download site. Alternate anti-virus applications may be used if approved. Download and run the current version and/or download and install anti-virus software updates as they become available.
2. NEVER open any attachments to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "purge" the deleted attachments by emptying your Trash.
3. Delete spam, chain, and other junk email without forwarding, in concert with UNLV's *Acceptable Use Policy* and the *Email Usage Policy*.
4. Never download files from unknown or suspicious sources.
5. Avoid direct disk sharing with read/write access unless there is absolutely a personal or business requirement to do so.
6. Always scan a floppy diskette or USB drive from an unknown source for viruses before using it.
7. Always back-up critical data and system configurations on a regular basis and store the data in a safe place.
8. If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications or any media that could transfer a virus, e.g., email or file sharing.
9. Multiple new viruses or variants of old viruses are discovered on most days. It is a very good practice to manually check for updates.