Estd.1962

NAAC "A" Grade

SHIVAJI UNIVERSITY, KOLHAPUR

MAINTENANCE MANUAL

Index

CHAPTER 1
Maintenance

1.1 Introduction

Building maintenance is work undertaken to keep, restore or improve every facility i.e. every part of a building, its services including Horticulture operations to a currently acceptable standard and to sustain the utility and value of the facility.

The objective of maintenance is: -

(i)   To preserve machinery, building and services, in good operating condition.

(ii)   To restore it back to its original standards, and

(iii)   To improve the facilities depending upon the development that is taking place in the building engineering.

In spite of recent improvements in building technology all the buildings deteriorate from the time they are completed. The rate of deterioration depends upon a number of factors. Not all the factors are under the control of the occupants. During the design and construction stages, the following become essential: -

(i)   Right choice of material.

(ii)   Suitable construction techniques.

(iii)   Adequate specifications for construction and installation work.

(iv)   Effective supervision throughout construction and rectification of defects prior to final certification.

(v)   Provision of adequate space for landscaping with proper design.

In fact the Shivaji University, Kolhapur provide for obligatory maintenance by the original contractor in the initial stages for a period of six or three months, depending upon the nature of the work, immediately following the date of completion as there are bound to be teething troubles in any new construction. If these are attended to, the maintenance pressure will be reduced. Where there are inherent defects both in design and construction the maintenance cost raises disproportionately to a higher level and the anticipated life of building is reduced.

Maintenance aims at effective and economic means of keeping the building and services fully utilizable. It involves numerous skills as influenced by occupancy and the performance level expected of a building. Programming of works to be carried out to keep the building in a good condition calls for high skills. Feedback from maintenance should also be a continuous process to improve upon the design and construction stages.

In the Manual wherever the maintenance of building is referred, it will include the associated services also.

1.2   Maintenance Services:

These include primarily operations undertaken for maintaining proper condition of buildings, its services and works in ordinary use. The use for which buildings are designed is a prime factor in determining the requisite standard of care.

Excessive maintenance should be avoided. At the same time, maintenance should ensure safety to the occupant or the public at large and should comply with the statutory requirements. The need also depends upon intensity of usage.

The repair works are classified in under mentioned categories:

Day to day repairs/service facilities

Annual repairs

Special repairs

In addition to above the following works are also executed by the maintenance wing of Shivaji University, Kolhapur as per guideline prescribed by Government of Maharashtra.

1.2.1   Day to Day Repairs

Day to day repairs are carried out by Engineering section in all the buildings under its maintenance on the basis of day to day complaints received

1.2.2   Annual Repairs

To maintain the aesthetics of buildings and services as well as to preserve their life, some works like white washing, distempering, painting, cleaning of lines, tanks etc. are carried out periodically.

1.2.3   Special Repairs

Such works are undertaken to replace the existing parts of buildings and services which get deteriorated on ageing of buildings. It is necessary to prevent the structure & services from deterioration and restore it back to its original conditions to the extent possible.

1.2.4   Additions and Alterations

The works of additions/alterations are carried out in buildings to suit the special requirements of occupants for functional efficiency. The facilities are updated by carrying out such works.

1.2.5   Preventive Maintenance

Preventive maintenance is carried out to avoid breakdown of machinery and occurrence of maintenance problems in buildings and services. Works of preventive maintenance are carried out on the basis of regular inspection/survey.

1.2.6 Maintenance of Bungalows (Hon'ble vice chancellor, Pro-vice chancellor and Registrar)

Shivaji University, Kolhapur is maintaining campus these includes Hon'ble vice chancellor, Pro- vice chancellor and Registrar, residences etc. Special Care has been taken for maitainence of above residences.

1.3   Means of effecting maintenance
1.3.1   Repair estimates

Annul repairs and maintenance estimates for building and Services are prepared as per requirement in the beginning of the year. The estimates cater to day to day repairs and annual (periodical) repairs and should include the whole expenditure on cost of labour (regular work- charged staff and on muster roll), cost of materials required for day to day works, cost of work being carried out through work orders and contracts, municipal and other taxes, if any, payable by the Government /party, anticipated to be incurred the maintenance of buildings in question. The total estimated cost of maintenance of buildings/structures during the year should be within the prescribed limits as approved by the body concerned from time to time both for annual repairs and special repairs.

1.3.2   Engineering Section/Substation

Shivaji University, Kolhapur has been assigned for receipt and disposal of maintenance complaints which are made by the occupants. Usually Junior Engineer is in-charge of the above sections.

1.3.3 Modalities of maintenance

The maintenance works are undertaken through one of the following:-

(i)   Directly employed staff

(ii)   Through Contracts

Whether the work should be carried out through contract or own work force is decided on the nature of the following: -

(a)   Type of work

(b)   Amount of work

(c)   Expediency or urgency.

i) Through directly employed labour:-

Directly employed labour is the most appropriate for routine day to day maintenance. This comes under the following two categories:-

Departmental labour: The cost of establishment due to workers such as their pay, allowances etc. are directly charged to the maintenance work.

In future there would be no further recruitment to the categories of Blacksmith and Upholster. The existing incumbents of these two categories will however continue to hold their respective posts, till vacated on account of promotion, resignation, termination of service, retirement, and death or otherwise.

The rounding off should be done at the level of Sub-division and a fraction of less than half ignored and half or more than half treated as one.

ii)   Through contracts

The annual repair work such as white washing, painting, petty works such as replacement of glass panes, repairs to plaster, changing roof tiles etc. are generally carried out through contract. The special repair works such as regarding, laying of water proofing treatment, repair of water supply pump sets, equipment's and accessories of A/C plants, Audio/Video conference systems, substation equipment's,

DG sets lifts are of good magnitude in financial terms, hence these are generally carried out through contracts.

1.4   Register of Buildings

Engineering section should maintain a Register of buildings up to date. The Engineer I/c. should certify to that effect at the end of every financial year after ensuring that necessary additions in the cost and in structures are made up to date. This certificate should be furnished by him to the Registrar every year in the month of July.

1.5   Safety of Buildings

(i)   All Buildings/structures are required to be inspected once a year by the Junior Engineer in-charge to ensure that the building/structure is not unsafe for use. In case of electrical and other installations, the Deputy Engineer (Electrical) should inspect the same and record a certificate to that effect. The Junior Engineers are also required to inspect such structures/installations twice a year and record certificates to that effect.

(ii)   In case of any deficiency found in the structure/installation necessary report should be made to higher authorities and immediate steps taken to get the same inspected by the Deputy Registrar (Civil) and further action taken to remedy the defects. The Divisional officers will also inspect important buildings/Gardens once a year. He shall bring to the notice of his Building and works committee cases where he   has   reasons   to   doubt   the   structural   soundness   of   any building/structure/installations and the latter will take such action, as he considers necessary.

(iii)   In case it is decided to demolish such unsafe building, it should be disposed of w i t h o u t   land by auction under the powers vested in competent authorities.

1.6   Cleanliness in the Campus

Cleanliness will be maintained in the Campus. Malba accrued from the execution of repairs in residences/buildings will not be allowed to stay at the place of work. Suitable points will be identified in the localities where malba generated from the day to day work will be stored by the departmental workers or the workers of contractors. It will be ensured that after work, malba is collected from the work place and deposited at the identified spot. Suitable provision will be made in the agreement for lifting of malba periodically from this identified spot. Safeguard will be taken that occupants do not throw garbage on this malba otherwise it would create unhygienic conditions for the residents.

Any leakage from the water supply line, sewers or unfiltered water supply line noticed in the campus will   be repaired immediately. Water   will not be allowed   to stagnate   on the roofs, courtyards, road side to act as breeding place for mosquitoes.

All precautions should be taken to keep the colonies neat and clean. In case unhygienic/health hazardous conditions are noticed in the portion of areas/service maintained by local bodies, the same will be reported to them and pursued for action. Overhead tanks will be provided with lockable covers and Mosquito proof couplings. The occupants will be advised against storage of water in coolers not in use and apply Mosquito repellants in the Cooler's pads etc. to check spread of Malaria.

1.7 Monitoring of maintenance

For effective maintenance and achieving client satisfaction; it is necessary to monitor the maintenance complaints at various levels.

CHAPTER 2
Engineering Section

2.1 Complaint Register

Complaint Register is an important document maintained at engineering section. All complaints received at engineering section are entered in the Complaint Register (Annexure-1) and these are closely watched to ensure that the complaints are attended to as expeditiously as possible. There may be different registers for different disciplines for the convenience of concerned Junior Engineer/Garden superintendent.

For maintaining the Complaint Register

(i)   Every complaint shall be assigned a serial number. Time of lodging of complaint shall be invariably recorded by the Receptionist. The complainant shall be intimated the complaint number and the likely time frame for attending the complaint for his reference.

(ii)   All complaints shall be entered in the register. Civil, Electrical complaints shall be entered in different registers.

(iv)   First entry in the complaint register on any day shall start on a new page.

(v)   As far as possible, the occupants shall be asked to indicate the nature of complaints to the attendant at Service Centre, so that the right person is deputed for the job and he carries with him necessary tools and materials. In many cases, the complaints are vague and the workmen have to make more than one trip to the house, to find out the nature of work and the tools and materials required. This wastage of man power should be avoided.

(vi)   Occupants shall be advised to register their complaints invariably with the Engineering Section. The Occupants may be advised to approach the senior officers in the Department only in cases where the complaints are not attended to within a reasonable time or the work has not been done satisfactorily. They shall be asked to quote the complaint number and date, so that the complaint could be investigated.

2.2 Disposal of Dismantled Material

Maintenance is a continuous process and lot of dismantled material is generated in this process. Dismantled material should not be allowed to be accumulated in large quantity and for more periods.

It occupies lot of valuable space in the engineering section, which otherwise could be put to use for storing serviceable material. Dismantled material when stored for longer duration gets deteriorated and loses its worth. Thus, in addition to blockage of space it causes revenue loss to the University by way of less realization of sale proceeds of the dismantled material.

Also it gives unsightly look as the dismantled material is seen scattered in the compound of Engineering Section. Most of the dismantled material can be survey reported by the Dy. Registrar (C i v i l). It is the responsibility of J u n i o r Engineer that Survey Reports of the dismantled material are sent to Dy. Registrar (Civil) periodically in time and ensure that valuable space at the Engineering Section is not occupied.

CHAPTER 3
Day-Day and Annual Repairs

3.1   Day to day repairs

Day-Day repairs are carried out by Shivaji University, Kolhapur in all the buildings under its maintenance. The works which are to be attended on day to day basis such as removing chokage of drainage pipes, man holes, restoration of water supply, replacement of blown fuses, repairs to faulty switches, watering of plants, lawn mowing, hedge cutting, sweeping of leaf falls etc. are attended under day to day service facilities. The purpose of this facility is to ensure satisfactory continuous functioning of various services in the buildings. These services are provided after receipt of complaint from the users at the respective engineering section Complaints of periodical nature like white washing, painting etc. which are usually got attended through contractors and cannot be attended on daily basis is transferred to register of periodical repairs.

3.2   Annual Repairs

The works of periodical nature like white washing, colour washing, distempering, painting etc. are called annual repair works and these are generally undertaken through system of contracts.

The periodicity of applying white washing and colour washing for a building has been laid down by the Government. The periodicity is two years for white washing and colour washing and three years for painting. In addition, works such as patch repair to plaster, minor repairs to various items of work, replacement of glass panes, replacement of wiring damaged due to accident, replacement of switches, sockets tiles, gap filling of hedges/perennial beds. Replacement/Replanting of trees, shrubs, painting of tree guards, planting of annual beds and trimming/pruning of plants etc., which are not emergent works and are considered to be of routine type, can be collected and attended to for a group of houses at a time and particular period of financial year, depending upon the exigency. Such works can be done under day to day repair also.

Following guidelines shall be followed for planning and execution of Annual repair works.

(i)   The total estimated cost of maintenance of a building/ structure during a year shall be within the prescribed limits as approved by the Government from time to time, for Annual repairs.

These may be suitably increased by the approved maintenance cost index in the relevant year.

(ii)   Programme for carrying out annual reports shall be drawn up at the commencement of each financial year.

(iii)   The annual survey of the buildings shall be such as to highlight defects of structural nature in the buildings which require personal investigation by the Dy. Registrar (Civil).

(iv)   The entire exercise of finishing under annual repair should be carried out in a professional manner. Before sanctioning of estimate/invitation of tenders, it should be ensured that all defects like dampness of walls, damage to RCC, brick work and plaster are removed in advance, so that the building looks renovated and presentable for sufficient time after annual repairs.

(v)   Payment for annual repairs is generally made on the basis of standard measurements and as such, there should not be lack of supervision on the part of the Departmental Officers. The Junior Engineer shall make it a point to physically inspect 100% of the buildings where annual repairs are to be carried out. The Dy. Registrar (Civil) shall carry out personal inspection to the extent of 50% and 25% respectively. The JE shall maintain a register indicating the number of residences where annual repairs are to be carried out, dates of his inspection and his observations regarding the quality of the works. The results of the inspection of the Dy. Registrar (Civil) shall also be recorded in the same register.

3.2.1   Register of periodical repairs

Complaints of periodical nature like white washing, painting etc. which are usually got attended through contractors and cannot be attended to on daily basis are transferred to this register. From this register/records of the particular premises appropriate information shall be passed on to the complainant about the admissibility of the request and the likely time it shall require for the compliance. (Annexure-5)

CHAPTER 4
Special Repairs

As the building ages, there is deterioration to the various parts of the building and services. Major repairs and replacement of elements become inevitable. It becomes necessary to prevent the structure from deterioration and under wear and tear as well as to restore it back to its original conditions to the extent possible.

The following types of works in general are undertaken under special repairs

(i) White Washing, Colour washing, distempers etc., after completely scrapping the existing finish and preparing the surface afresh.

(ii) Painting after removing the existing old paint from various members.

(iii) Provision of water proofing treatment to the roof. All the existing treatments known are supposed to last satisfactorily only for a period of about ten years.

(iv) Repairs of internal roads and pavements.

(v) Repairs/replacement of flooring, skirting, dado and plaster.

(vi) Replacement of doors, window frames and shutters. Replacement of door and window fittings.

(vii) Replacement of water supply and sanitary installation like water tanks, WC cistern, Wash basins kitchen sinks, pipes etc..

(viii) Re-grassing of lawns/grass plots within 5-10 years.

(ix) Renovation of lawn in 5-6 years.

(x) Replanting of hedges in 8-10 years.

(xi) Completely uprooting and removing hedges/ shrubbery.

(xii) Replanting of
   a) Rose beds in 5-6 years.
   b) Perennial beds in 5-6 years.
   c) Canna beds in 1-2 years.

(xiii) Shifting of any garden feature from one site to another within building.

The building services fixtures including internal wiring, water supply distribution system etc. is expected to last for 20-25 years. There afterwards it may be necessary to replace them after detailed inspection.

Electrical special repairs in general are whole sale replacement of the wiring and the electrical installations. Earthling is also to be attended. Life of various Electrical Equipment's/installations etc.,

The expected economic life of the building under normal occupancy and maintenance conditions is considered to be as below:

(i)	Monumental buildings	100 years.
(ii)	RCC Framed construction	75 years
(iii)	Load bearing construction	55 years.
(iv)	Semi-permanent structures	30 years
(v)	Purely temporary structures	5 years

The life of the building mentioned above is only indicative and it depends on several factors like location, utilization, specifications, maintenance and upkeep/care• taking.

The replacement, renovation and major repairs become inevitable as the life of all the components are not identical.

All the three categories i.e. day - day, annual and special repairs/services are interrelated. Neglect of routine maintenance and preventive measures lead to more extensive periodical maintenance and in the long run major repair or restoration which could have been avoided or postponed.

4.1   Register of special repairs

Complaints of special nature repairs, which cannot be attended on daily basis, shall be transferred to this register. The special repairs to buildings shall be divided in following six groups: (Annexure-4)

(i)   Concrete work.

(ii)   Masonry works including plaster, flooring and brick work.

(iii)   Wood work.

(iv)   Steel work.

(v)   Sanitary and Water supply.

(vi)   Water proofing treatment.

(vii)   Electrical wiring and fittings

Few pages shall be allotted separately to each of these groups in the register and an index shall be prepared in the beginning of the register. The complaint of special repair nature shall be transferred from the complaint register to the relevant group in this register. All details about the complaint shall be properly filled in the columns of the register.

4.2 Authenticity of Special Repairs

Any work of Special Repair to be undertaken in the division has to be certified by the Dy. Registrar (Civil). The Dy. Registrar (Civil) has to verify himself the necessity of undertaking Special Repair to any item of the building. Estimates of Special Repairs of course, will be initiated by Junior Engineer but Dy. Registrar (Civil).Before accord of approval at his level or sending it to higher authorities will record in writing in the body of the estimate that the necessity has been verified by him.

There should not be too many estimates for Special Repairs in a subdivision. As far as possible, number of estimates should be restricted to number of identified subheads as indicated in the register of Special Repairs. In that case it may be possible that one Special Repair Estimate is operated by more than one JE in the subdivision.

4.3 Extra Ordinary Special Repair

When expenditure on Special Repair to a particular building is in excess of the permissible yardstick of Special Repair, the same come under the category of Extra Ordinary Special Repair. Expenditure on Special Repair up to permissible li mi t can be incurred by the Dy. Registrar (Civil) beyond the permissible limit however Dy. Registrar (Civil) has to have the approval of the higher authorities.

CHAPTER 5
Additions/Alterations

Two types of Additions/ Alterations are carried out in non residential buildings. Addition/ Alterations are to be carried out to suit the special requirement of occupying department for functional efficiency. Such works of Addition/ Alterations are carried out at cost of occupying department after ascertaining the technical feasibility. Some Addition/ Alterations are carried out by Shivaji University, Kolhapur themselves as a general requirement for better functioning of offices located in the office complex. In case of residential buildings, some Addition/ Alterations are carried out by Shivaji University, Kolhapur keeping in view the safety of buildings, approach to buildings, augmentation of services etc. Which are beneficial to all residents in general works of addition/alterations are also carried out in residences at the request of occupants for providing facilities in the residences which otherwise are within the yardstick of facilities for those type of quarters but were not provided at the time of original construction. Such Addition/ Alterations are carried out on payment of certain percentage of estimated cost of providing the facility. (Annexure-6)

No additions/alterations once carried out to any Govt. residence except temporary prefab works purely related to special security aspects shall, however, be removed upon the vacation of these houses by the "allottee concerned. "
Under mentioned points shall be observed while carrying out addition/alterations in government buildings:

(i) No addition/alteration shall be carried out to permanent public buildings without the concurrence of the Chief Architect/Senior Architect in writing except for the amenities like provision of wash basin or sink etc.

(ii) The allottee shall be asked to fill up a form as at Annexure-11. Counterfoil of the form shall be returned to the allottee duly signed by the acknowledgement of the receipt of the application.

(iii) The work of addition/alteration shall not be taken up as a matter of rule but as exception since the availability of resources is limited.

(v) 'No non-usability' certificate in respect of houses where works of addition/ alterations have been taken up at request of allottee shall be issued except when such works render the house really unusable.

Works of additions/alterations on Horticulture s i d e can be carried out at the request of occupants depending upon t h e requirements. Such works are: -

i) Changes in length and design of hedges, shrubbery, planting beds and rockeries etc. Making some Changes in basic design of gardens/lawns by providing Mounds, undulations, rockeries etc.

ii) Providing some garden structures like pergolas, arches, GI pipe frames shelters, seats and water body etc.

iii) Digging of new tree /shrub pits, planting beds within existing garden area or changing the situation of beds, kitchen garden, lawns etc.

In Horticulture, the works of additions and alterations shall be carried with the approval of competent authorities as per the powers delegated to them and on availability of funds.

Timely communication and coordination shall be made by the discipline if their work taken up by it is likely to affect other disciplines.

CHAPTER 6
Preventive Maintenance

Preventive maintenance is carried out to avoid the breakdown in case of machinery or occurrence of maintenance problems in buildings and services. In case of buildings preventive maintenance against seepage for example, is necessarily to be carried out. Preventive maintenance however depends largely on routine inspection/survey of the buildings.

6.1 Accessibility for Maintenance

It is necessary that the place to be maintained is capable of being reached for maintenance to be carried out. Access varies from day to day needs to access for a trained and experienced man to attend to a maintenance problem.

In some of the structures regular shafts have been provided for water supply and sanitary installations. The shafts are too tight and there is no working space for workman. The problem is compounded by inadequate light in the shafts. Not only the elbow space has not been provided but there is no working platform for workman. The workmen refuse to attend to leakages and repair pipe lines in such circumstances. It is necessary to provide shafts with access/working platform for the work men to attend to repairs.

Replacement of glass panes in the windows have become another problem. In general the windows open outside and putty is also placed accordingly. In addition, for residential buildings, grill work is provided for safety of residents. The windows have generally a full sized glass sheet as a result it has become difficult to replace and even clean these glass panes. The problem is acute in buildings beyond three story's. It is necessary to provide proper accessibility to these windows through a regular arrangement in such a manner as to ensure fixing of glass and their cleaning from inside of the building, maintenance and upkeep of desert cooler & WTAC u n i t s installed at the windows.

Overhead tanks have been provided over the buildings. With a view to keep the roof inaccessible for the residents, no terrace staircase has been provided to reach the terrace. In the day to day maintenance, however the maintenance staff are called upon to go to the terrace to check the over flow and the like for which regular access IS necessary. Ladders should be provided as a means of access, preferably on a permanent basis.

Buildings of monumental nature are finished with special treatment on roof, false ceiling, wall panelling and carpetting on wall which may require to be attended. It is necessary to have permanent arrangements for reaching such heights as a part of maintenance tools. It can be a dismantlable tubular scaffolding system provided with rollers as a standby for reaching the false ceiling.

6.2 Inspection of buildings and services
6.2.1 Periodical inspections
(a) Buildings and services

The starting point of maintenance to building is the regular inspection of buildings. It should be carried out periodically with a view to keep down the restoration cost to the minimum and to attend to essential repairs at the opportune moment. The symptoms of malfunctioning varies from building to building and the resulting deterioration varies with reference to the climatic conditions, pollution, fungi, the insect attack, subsidence, flooding, intensity of usage, careless usage and the like.

It is necessary to know when the building should be inspected, what should be inspected, at what level of deterioration a component should be replaced or repaired and whether any preventive maintenance is called for.

As per Shivaji University, Kolhapur Citizens' charter and guidelines issued by Government, programme for maintenance work for the ensuing year is to be finalized by 30thApril of the year. To achieve this it is necessary that all buildings should be inspected by the JE in March and April. In general, the Overseer should inspect each and every building under his charge once every six months, the Junior Engineer once a year and the Dy. Registrar (Civil) should inspect all buildings where serious defects have been brought to his notice. In case there are doubts about structural soundness of a building, the same should be brought to the notice of Building Works Committee on a priority basis so as to take prompt remedial action. In fact, safety of the building is given a primary place and for this purpose, structural soundness is the most important requirement of the building.

There is necessity to ensure and maintain uniformity for objective inspection of the buildings as it is difficult for every member of staff to know what should be inspected.

These reports help in the following

(i)   Preparation of a need based estimates for annual, special and extraordinary repairs of buildings.

(ii)   Preparation of programmers for undertaking major repairs according to an established programme bringing minimum inconvenience to the residents/ occupants.

(iii)   A regular inspection prevent/for stalls an unexpected break-down of a building this becomes necessary as we have to maintain building even beyond their normal life period

Inspection should also cover outside areas such as the drive ways, paths, lawns, gardens, hedges, trees, boundary walls, functioning of treatment plants provided if any in the form of septic tanks etc.

It is necessary to inspect all storm water drainage works before and during monsoon periods.

Any item pertaining to Civil/Electrical in garden area such as broken man-holes, Drains, water pipe lines, Cable etc. which needs repair should be reported to concerned Dy. Registrar (Civil)

(b)   Electrical Installations

The Shivaji University, Kolhapur maintains the installations and services at the office and residences of VIP/VVIP including all arrangements made during functions held on their behalf at University campus. These inspections/instructions do not supersede the normal/periodical/routine checks which are required to be carried out on the equipment's and installations like insulation tests, Earth tests, Oil tests, Replacement of component schedule, oil replacement, other tests to be carried out as per manufacturer's recommendations, but are in addition to the same.

6.2.2   Inspections for taking over of buildings

Buildings along with their services are designed and constructed to meet specific user requirement. So as to ensure full user satisfaction, it is necessary that the buildings and services on their completion should be subjected to intensive review by the team of construction and maintenance Engineers.

During the course of construction, certain tests and checks are carried out by the engineer-in-charge of the construction.

Also whenever any works are entrusted to contracting agencies, these are tested and taken over by the Engineer-in-charge. Certain guarantee e certificates from the suppliers/manufacturers are also received by Engineer-in-charge before accepting materials a n d e q u i p m e n t ' s . Maintenance in charge should ensure that these are handed over to him at the time of handing over of facility.

6.3   Preventive maintenance

As mentioned above, for carrying out preventive maintenance, inspection of building has to be carried out. The building is to be inspected during the months of March-April and September-October. Monsoon winds bring rainfall to Maharashtra

i) South West Monsoon (June-October)

Experience has taught that monsoon rains, winds and cyclone cause considerable damage to buildings, tall structures, uproot trees and lamp posts, cause floods, roof leakage into buildings, blow water through broken window panels, blow off thatched

Roofs, hutments and bus shelters, cause disruptions in power supply, water supply and sewerage systems resulting in untold sufferings to people besides causing huge financial , losses to the ex chequer and endangering lives. To minimize such losses and avoid danger to life it is necessary to undertake some specific pre-monsoon preventive measures which are briefly discussed below :

6.3.1   Attending to services before Monsoon Rains/Cyclones.

Buildings and Services are to be thoroughly checked for safety and functioning before monsoon. In coastal areas the same are checked before cyclones. Precautionary measures are to be taken for various items of the buildings/services, some of which are mentioned below:

a) Temporary Roofing

Many buildings are provided with temporary roofing like AC Sheet roofing. Before the onset of the monsoon, the Engineer-in-charge of Maintenance should see that the L/J hooks, bitumen washers, Limpet washers are in position. Precautionary measures against blowing off the roof should be taken by lightly loading the roof temporarily or providing MS flats/rods fixed by bolts and nuts to purlins for rows of AC Sheets.

b) Door /Window glazing :

All broken glazing should be replaced and sufficient number of glass window panes and iron monger fittings should be kept in stock for emergency repairs. The tower holts, hooks and eyes and other wind appliances should be made in working condition. Occupants should be advised to keep the doors and windows closed during cyclonic weather especially at nights.

c) Checking buildings against seepage

Terraces of all the buildings may be inspected well ahead of the monsoon rains in June and December and necessary repairs carried out. The roofs should be cleaned and debris removed from the roof to avoid blockages in roof gutters and rain water pipes. Rainwater inlets should be checked and ensured that there are no damages around these. Vertical rain water pipes should be properly clamped to the walls. Seepage through cracks developed over Chajja is very common. It should be ensured that required repairs are carried out to the junction of Chajja with the walls.

d) Checking of external areas

Open areas and lawns should be inspected and measures taken to ensure that rain-water does not accumulate therein. Wherever storm water drains are under the maintenance of Shivaji University, Kolhapur the same should be desilted and paved surfaces or bunds repaired. Precaution should be taken against erosion of land and embankments.

e) Checking of sewers and sewage installations

All inspection chambers, manholes and sewer lines should be cleaned and flushed to establish free flow of sewage. Sewage sumps should be cleaned of accumulated grit, sand and sludge. Bunds of oxidation ponds should be strengthened wherever necessary.

f) Checking of electrical installations

Because of rise in ground water table at places, it may be necessary to remove electric pumping sets installed in wells and sump, below ground water level and raise them temporarily to safe levels. Care should be taken to ensure availability of stand• by power supply arrangement to take care of breakdown in power supply in monsoon or at the time of cyclones. The Diesel Generating sets should be checked and kept in working condition and wiring should be checked for loose connections.

g) Checking of Air-conditioning installations

Wherever Central AC plants or package units are provided, the dehumidification system consisting of strip heaters, humidistat etc. should be checked for their functioning.

6.3.2 Post monsoon/cyclone measures

Inspire of pre-monsoon measures taken by various buildings/services, very often these are affected during the monsoon and cyclones. In coastal or cyclone prone areas, the services are affected more. Immediately after monsoon, all important structures/services should be inspected by a team of engineers from all disciplines concerned with the maintenance and work should be planned to put the services in order immediately.

Overhead cables, uprooted light poles, restoration of power supply, disinfecting of water supply lines/installations, ensuring normal water supply, restoration of sewage pumping operations, flood relief works, repair to breaches to embankments of roads and bunds are some of the important areas which are to be attended immediately after monsoon/cyclone. Detailed inspection of the buildings should be carried out to ensure that broken false ceiling, broken glass panes, blown off A.C. sheet roof, claddings, doors and rolling shutters etc. are attended immediately.

Where breakdown would result in serious damage to the equipment and costly repairs. preventive maintenance is necessary. Whereas Preventive maintenance is also justified where it improves performance and the cost is less, compared to cost of repair after a failure.

The works of preventive maintenance in case of buildings are to be carried out latest by 15th June and 31st October. In case of periodic inspection machinery equipment is carried out to avoid the conditions leading to breakdown or harmful depreciation. It is also carried out for proper up-keep of Plant through servicing and repairs while they are still minor. However in case of machinery and equipment's, frequency of inspections should be decided and the system should be designed for improved maintenance techniques, low cost maintenance and avoiding the over maintenance on the basis of statistical data available for maintenance and manufacturers recommendations.

Engineering Section…………………… <u>M/C Numbered</u>

COMPLAINT REGISTRATION FORM

1.   Flat No.

2.   Name of the allottee

3.   Nature of Complaint

Date   ……………..

Signature & Name of the complainant

………………………………………………………………………………

Received Complaint for Flat/Quarter No. …………….. <u>M/C Numbered</u>

Date …………………………….

Signature of Enquiry Clerk/ JE/Receiving Officer

ACKNOWLEDGEMENT T O   COMPLAINT

No ....

　Dated :..........

To

　　　Ref:　　Your　Complaint No. ....　　dated .... For Flat/Quarter No .....

Dear Sir,

The subject complaint is acknowledged Necessary action is being taken to fix-up an agency for attending to the same.   We will revert back to you no sooner we are in a position to take up the   subject complaint. I request you to   kindly   bear with us.

However, the complaint is likely to be attended in next .... months.

　　　　　　　　　　　　　　　　　　Yours faithfully,

　　　　　　　　　　　　　　　　　　(Junior Engineer)

.

WORKERS NOTE BOOK

Sr. No.	S.No. of complaint	Flat/Quarter No. and Colony	Nature of Complaint	Details of work done	Balance work, if any	Sign. Of worker	Sign of occupant	Remarks
1	2	3	4	5	6	7	8	9

REGISTER OF SPECIAL REPAIRS

Special Repair Group _____

Sl.No.	Complaint No.	House No./ Locality	Location of Repairs	Approximate Quantity	Repairs required in			Schedule of Repairs
					Less than 1 month	Within 3 months	Within 6 months	
1	2	3	4	5	6	7	8	9

REGISTER OF PERIODICAL REPAIRS

| Sl. No. | Complaint No. | House No./Locality | Request re ardin2 | | Due/ Not due | Date planned for the work | Date of intimation to allottee | Date of completion of work |
			White washing/ Distempering , Fans cleaning, Surface Dressing of lawn, Vegetation cleanin etc.	Door/window Painting, Painting of fans,D.B. Open metal conduits etc.				
1	2	3	4	5	6	7	8	9

APPLICATION FOR ADDITIONS/ALTERATIONS I N GENERAL POOL ACCOMMODATION

PART A : TO BE FILLED BY THE ALOTTEE :

I. Name ....

2. Designation ....

3, Office Address : ....

4. Residential Address: ....

5. Type of Accommodation in which residing ....

6. Actual Date of occupation of present accommodation: ....

7. Particulars of works desired with location (Refer guidelines enclosed).

....

ACKNOWLEDEMENT

Received application dated ....for addition/alteration in Flat/quarter

No .... of colony ...., ...

Dated:...

Signature of Junior Engineer

(a)   Inspection of Buildings (Civil)

(a)   House no. and Type: (b)   Location:

(c)   Date   of   Last   (d)   Date   of   present   inspection
Inspection:

S.No.	Item	Needs Repair			Needs Replacement		Priority			
No.		Action	Quantity	Cost	Quantity	Cost	Immediate	Annual	Routine	Repairs
	2	3	4	5	6	7	8	9	10	
1.	**Walls**									
1.1	Cracks									
1.2	Repair to plaster									
1.3	Repair to brick work									
1.4	Dampness									
2.	**Floors**									
2.1	Cracks									
2.2	Settlement									
2.3	Slopes									
2.4	Skirting cracks									
2.5	Dados cracks									
3.	**Doors, Windows, Ventilators & Cupboards**									
3.1	Glass panes broken									
3.2	Panels in shutters broken									
3.3	Panels fit improperly									
3.4	Improper/missing fittings									

3.l.l   Hinges

3.1.2   Handles

3.1.3   Tower Bolts

3.1.4   Aldrops

3.1.5   Floor door stopper

3.1.6   Knobs

3.1.7   Cleats

3.1.8   Hooks& Eyes

3.1.9   Curtain Rods l.1.lO Stays

3.1.lO   Pelmets

4. Roofs

4.1   Leakages/Damp patches

4.1   Water proofing treatment

4.2   Golas

4.3   Khurras

4.4   Brick drip course

4.5   Rain water pipe

4.6   Regrading

4.7   Top Layer of tiles

4.8   Parapet, coping

5. Water Supply & Sanitary fittings

5.1   Leakages in pipe joint

5.2   Functioning of washers

5.3   Functioning of traps in fittings

5.4   Functioning of floor traps

5.5   Functioning of overhead/low level cistern

5.6   Air Locking

5.7   Leakages in pipe joints

5.8   Condition of overhead tank

5.9   Cleaning of overhead tank

5.I0   Fittings

5.10.1 Wash basin

5.10.2 Soap container

5.10.3 Mirror

5.10.4 Glass shelf

5.10.5 Towel rail

5.10.6 Hangers

5.10.7 Sinks

5.10.8 Taps

5.10.9 Pillar cocks

5.10.10 Showers

5.10.11 Cisterns

5.10.12 Ball valves

*5.*I 0.13   Seat cover

5.10.14   Step

6.   External Services

6.1   Manhole covers

6.2   Covers to gully traps

6.3   Cleaning of manholes

6.4   Plinth protection

6.5   Cleaning of storm water drain

6.6   Approach roads

6.7   Service lanes

7.   Finishing

7.1   White washing/colour washing/distemper

   (a)   When was it done last?

   (b)   When is it due?

   (c)   Existing condition.

7.2   Painting

   (a)   When was it done last?

   (b)   Existing conditions

   (c)   When is it due.

8. Common Areas

   8.1   Railing to staircase

   8.2   Staircase steps

   8.3   Staircase nosing

   8.4   Shafts

(b) Inspection of Buildings (Electrical)

(a)   House No. and Type: (b) Location:

(c)   Date of Last   (d) Date of present inspection:

     Inspection:

Sl.No.	Item No.	Needs Repair		Needs Replacement		Priority			
		Action	Quantity	Cost	Quantity	Immediate	Annual	Routine	Repairs

1. Switch Boards

1.1 Regulator

1.2 Switches

1.3 Fixing of tiles

2. Fans

2.1 Conopy fixing

2.2 Speed and noise

3. Socke outlet points and connection

3.1 Tile

3.2 Switch

3.3 Outlet connection if any

4. Fittings

4.1 Reflector

4.2 Louvers/Perspex cover

4.3 Suspension rod

5. Exhaust Fans

5.1 Speed and noise

5.2 Louvers

5.3 Connecting wires i/c. ceiling rose

6. Call bells

6.1 Bell push

6.2 Connecting wire

6.3 Ball Buzzer

7. Sub distribution boards/BDB/Main Board

7.1 Switch covers

7.2 Fuse Kit Kats

7.3 Earth connection

7.4 Fuse rating

7.5 Inter connection

7.6 Boards

<center>**(c) Inspection of buildings/gardens**</center>

(A) LAWN :

i) Weeding

ii) Patch repair

iii) Renovation

iv) Regressing

(B) HEDGE :

i) Gap filling

ii) Replacement

(C) PRUNNING & TRAINING

i) Naturally required pruning

ii) Pruning required for security

Purpose of building as well as occupant

(D) PLANTING BEDS :

i) Needs Replacement

ii) Gap filling

(E) U/F WATER SUPPLY

i) Matter to be reported to U/F Water

Division after inspection.

(F) ROCKERIES :

i) Gap filling of dead one

ii) Replacement of damaged, weak

iii) Replacement of stones

iv) Thinning, trimming

v) Redesigning of paths, Maintenance of paths

(G) KITCHEN GARDEN

i) Change in site

ii) Plan for planting of vegetables

(F) ROAD SIDE PLANTATION

i) Gap filling Nos.

ii) Trimming, pruning

iii) Tree Guards not required & to be removed/repair/painting etc.

iv) Proposal for new plantation, Digging of holes etc.

v) Misc.

vi) MOU-Detailed report(performance & financial achievements)   32

DRAFT ALLOTMENT LETTER

No._____   Allotment/Immediate

Shivaji University, Kolhapur

Establishment Department   Dated the

To

        _____

        _____

        _____

Dear Sir/Madam,

The marginally noted residence is hereby allotted to you in accordance with the provision of the 'Allotment of Govt. residences under the Central Rules, 1981. This allotment is made for the . period you remain attached to .... Division and function as ....in charge of ....Section/Sub-Division/Division.

l. Particulars of residence   2. Type

3. In lieu of unfurnished residence   4.Type

5. Furnished

2.   You are requested to send your acceptance within 5 days from the date of receipt/ issue of this letter. The acceptance should be in the enclosed form in duplicate and should be addressed to the undersigned (by name).

3.   If no acceptance is received within the prescribed period of 5 days, the allotment will be deemed to have been refused and your case will be deemed to have been refused and your case will be dealt with accordingly.

4.   If you are a temporary Govt. servant, you are required to furnish a surety bond from a permanent Central Govt. servant along with your acceptance. The bond should be on the

5.1f the allotment is accepted you should take possession of the allotted residence from the CPWD Enquiry Office concerned within 8 days of the date of receipt of this letter. In case of failure to take the possession within the time specified above, you will be liable to pay license fee with effect from the 8^{1}h day and the allotment shall be liable to cancellation.

                                                    Yours faithfully

                                            Deputy Registrar (Establishment)
                                              Shivaji University, Kolhapur
                                            Dated,

Copy forwarded to :

.......................Sub Division.

Cashier ....Division/Bill Asstt.

Accountant,............... Division

DRAFT ACCEPTANCE LETTER

Shivaji University, Kolhapur

Establishment Department

Sub: Acceptance of Residential Accommodation. Sir,

I accept the allotment of residence

No ....made   to   me   vide   your   letter   No .... dated

received by me on .... (dated).

Full details of my emoluments are given below :

i)	Pay	Rs ....
ii)	Special Pay, if any	Rs..........
iii)	Pension, and pension equivalent	Rs. ·········
	of Death-cum-Retirement gratuity.	
iv)	Dearness Pay, if any.	Rs ....
v)	City Compensatory Allowance	Rs...........
vi)	Any other allowance other	Rs..........
	than Dearness Allowance,	
	Conveyance allowance,	
	House Rent etc.	

<div align="center">Total</div>

Rs............

I am a quasi permanent/permanent Central Govt. servant.

I am a temporary Govt. Servant and particulars of my Surety are given below

i)   Name of surety ....

ii)   Designation of Surety ....

iii)   Office/Ministry where employed.

No other Govt. accommodation is allotted to me or to my Wife/Husband to date, either by the Directorate of Estates or by the Department of Rehabilitation or by any other Govt. Deptt./Autonomous body/Semi Govt./Public Undertaking Office.

I certify that I do not own a house or flat in the station of posting either in my own name or in the name of my wife/husband or any other member of my family. I also undertake to inform you if and when I or any member of my family acquire a house at this Station.

I agree to vacate the quarter within two weeks of my transfer from the present post, without. waiting for a formal allotment in general pool or otherwise.

I have carefully read the Rules regarding Allotment of Govt. Residences at the disposal of Shivaji University, Kolhapur to its Employees and hereby agree to abide by these rules.

<div align="right">Yours faithfully</div>

<div align="right">Signature Name in Block letters Designation</div>

<div align="right">.................Date.</div>

SURETY BOND

I, Shri ……………………….. son of Shri ……………………. . employed as …………………. In the ……………………hereby stand surety, which expression shall include my heirs, executors and administrators to the President of India (hereinafter call the Govt.) (which expression includes his successors and assignees) for payment of Shri ……………………. of licence fee and other dues in respect of the residence now allotted to him by Govt. as also for any residence, addl. Accommodation, extra servant quarter for garages that may be allotted to him from time to time by the Government.

2. 'I, the surety, shall indemnify the Govt. against all loss and damages until delivery of vacant possession of the same is made to the Govt. I, the Surety, hereby undertake to pay to the Govt. forthwith on demand by Govt., and without tenure all such sums as may be due to the govt., as aforesaid and I hereby agree that the Govt., sh3.Il be at liberty (and be hereby irrecoverably authorized to do so) to recover the said sums from the salary payable to me and the decision of the Govt., as to the amount so to be recovered shall be final.

3. The obligation undertaken by me shall not be discharged or in any was affected by an extension of time or any other indulgence granted by the govt. to the said, Shri ………………….(name of allottee) or by any other matter of thing whatsoever which under the law relating to sureties would but for this provisions have the effect of so releasing me from my such liabilities.

4. This guarantee shall not be discharged by my death nor shall it be recoverable by me at any time, except with the consent in writing of the Government, until the delivery of vacant possession of any such residence servant quarter or garage, which is in occupation of the allottee of the Government quarter.

5. Provided, however, that this guarantee shall inso-facto terminate from the date Shri…………………… is declared permanent or quasi-permanent in any service in the Government of India.

The Govt. have agreed to bear the stamp duty, if any, for this document. Signed delivered by said…………. …………… .

at New Delhi the day of …………………………………

(Signature of Surety)

Signature, address & Occupation of Witness

Designation…………

INSPECTION LIST NO. 1

Substation equipments, Generating Sets, Supply Co., Service Connection.

Place

Date of Check Name of JE(E)

Time of start

Time of completion

Division No

H.S. Voltage

S.No. Item

SUB STATION EQUIPMENTS   Position   Remarks
1.   General look of HT panels

2.   How many incoming and outgoing panels?

3.   How many in 'ON' position?

4.   When were the contracts checked last?

5.   When was the oil tested/replaced?

6.   When were the Relays Calibrated/tested?

7.   General cleaning of panel

8.   Functioning of Meters in panel

9.   If trickle charger is provided, state of the same and battery and Maintenance of Battery.

10.   Is there alternate Source of Supply and if so when was it tested?

11.   Has DESU/NDMC been informed in advance of the programme/function?

12   Are the voltage and supply and frequency within Limits of IE Rules. If not, any intimation given to supply Co.?

13   No. and capacity of transformers?

14   How many of them are in operation at a time?

15   How often the transformers are switched 'ON' and 'OFF'?

16   How often the tap changers have been used?

17   When was the oil tested and if found not in order.

18   General condition of transformer i/c oil leakages if any?

19   How often the transformer is cleaned?

20   Oillevel check

21   Silica Gel check

22   Bucholtz Relay check if provided

23   Heating/Temperature Rise

GENERATING SETS (SAND BY SUPPLY)

	Yes/No	Date

Change-over switch operated checked
(weekly)

Cable terminals connection checked

Cleaned/checked all terminals(weekly)

Generator operated

On no load

On connected loan

Driving/V- belt checked

Radiator filled/no leakage

Filters clean

HSD oil tank full

Mobil oil checked

Battery fully charged

Terminal checked

Distilled water checked

AMF panel-relays contacts, terminals

Checked and for its operation.
Stand by water filing arrangement is available

INSPECTION List NO. 2

Electrical installations, lifts, water supply pumps, sewage pumps, Filtration Plants.

Place:

Date of check :

Name of JE(E) :

Name of AE (E):

Division:

'A' Electrical Installations :

S. No.	Position	Remarks
1. Power outlets for metal detectors		
2. Power outlets for PA system		
(i) Normal		
(ii) Standby		
3. Power supply for AIR/Doordarshan		
4. Power outlet for car call system		
5. Power supply for security lights.		
(i) Main		
(ii) Stand by		
6. State of		
(i) Lamps		
(ii) Fittings		
(iii) Fans/Regulator		
(iv) Power/Light socket outlets		

Whether alternate source of supply available?
All cables test for insulation & healthiness
from substation to feed pillar/outlets.
9. (i) Cable connections, terminals checked.
   (ii) Overheating at joints?
10. Sub Distribution Boards checked for
(i) Cleanliness
(ii) All MCBs/MCCBs in working order
(iii) Neutral/earth properly connected
(iv) Signs for overheating/sparking
'B' Lifts
1. No. of Lifts
2. Make/Passenger capacity
3. Type (manual/automatic with or without Attender)
4. Type of control
5. No. of floors served
6. Whether under comprehensive/service

Name of Firm:
7. Operation
(i) Landing call buttons
(ii) Car buttons
(iii) Emergency stop

8. Functioning of all safety devices

9. Car light/fan

10. Intercom working & checked   Car to M/c Room

                                           Car to Control Room

                                           Car to JE Room

11. Condition of rope (s)

12. Condition of trailing cable

13. Condition of sheave

14. Governor functioning

15. Smooth/Jerkfee operation

16. Levelling accuracy

17. Doors opening key availability

18. Overload safety for Car

19. Last servicing done in machine room. Date

20. Proper illumination in the lift shaft

21. Seepage in the lift pit

22. Condition of Buffers

23. Working of limit switches

24. Proper lighting ventilation in M/c Room & proper approach

25. Proper illumination at all car landing

26. Operation of controller

27. Operation of floor detector

28. Whether switch available in the car to prevent any unauthorized person from operating the Lift in the case of attendant operated Lifts.

'C' Water Supply Pumps

1. No. of Pumps   (i) Electric Drive

                                      (ii) Diesel Drive

2. Make, H.P. of each

3. Rated current

Current actually drawn

4. Voltage at terminals

5. Type of starter

6. Foot Valve O.K.

7. Priming arrangement

8. Condition of flexible coupling

9. Greasing of bearings

10. Vibration of Motor

11. Overheating of Motor

12.No. of hours normally run

13. Sump water level indicator

14. Pressure at pump delivery

'D' Sewage Pumps

1. Type of Pump

2. Make

3. H.P./rated current

4. Current actually drawn

5. Type and condition of Starter

6. Last service on:

'E" Filtration Plants

1. Type of Plants

2. Make

3. Medium used for filtration

4. Frequency of change of filter medium

5. Motor H.P./rated current

HANDING /TAKING OVER OF BUILDINGS & SERVICES

FORMAT FOR HANDING OVER/T AKING OVER OF COMPLETED BUILDINGS INCLUDING SERVICES

1. Name of work/location
2. Salient details of the building
    a) Type of Structure
    b) Plinth area-floor wise
    c) Type of Foundation
    d) Special treatments/linings
    (i) Acoustic treatment
    (ii) False floors
    (iii) Special type of flooring
    (iv) False ceiling
    (v) Vapour barrier treatment
    (vi) Under deck/Over deck insulation

W/S and Sanitary installations

(a) Water Supply
(i) Sources of W/S to the building and source wise capacity
(ii) Brief specification of W/S distribution system

(b) Details of tube wells if any
(i) No. of tube wells
(ii) Yield of each tube well
(iii) Type of boring and depth
(iv) Brief specifications of boring pipes

(c) Type of w/s distribution
(i) OH tank details like material, lining, height, capacity etc.
(ii) W/S Sump details like material, Depth,capacity etc.

(d) Sewerage System
(i) Specification of Sewerage System
(ii) Out fall of Sewerage System
(iii) Sewage Sump details if any
(iv) Sewage treatment plant details if any

4 Electrical and Air Conditioning System
(i) Details of internal electrical installations like wiring etc.
(ii) H.T. and L.T. Pannels details
(iii) Type of fans
(iv) Whether the building is centrally Air Conditioned.
(v) A.C. Load
(vi) Type of plant
(vii) Brief specifications

5 Firefighting/Fire alarm system
(i) Type of firefighting system
(ii) Type of fire alarm

(iii) Location of control room
(iv) Brief specification of firefighting system
(v) Brief specification of fire alarm system
(vi) Fire tank capacity
(a) Over Head tank
(b) Under Ground tank
(vii) No. of fire hydrants
(viii) Fire pumps no.,& Capacity.

6 Details of Guarantee/Warranty
certificates obtained for building
for various services/treatments

7 Contract details
(a) Name of the building
contractor & Address
(b) Agreement
(c) Completion period
(i) Commencement date
(ii) Date of completion
(d) Approximate completion cost
(a) Building
(b) W/S and Sanitary
(c) Electrical and Air-conditioning

8. Major defects noticed at the time
of handing over/taking over
(a) Building work
(b) W/S and Sanitary installations
(c) Electrical and A/C works

9. Handing over of Completion drawings(4 sets of each)
(a) Architectural Drawings Nos.
(b) Structural Drawings Nos.
(c) Water Supply, Sewerage & Drainage
Drawings Nos.
(d) Electrical & AIC drawings Nos.

Handed over	**Taken over**
Signature:	Signature:
Name:	Name
Designation	Designation:

MAINTENANCE NORMS, FREQUENCY OF APPLICATION OF FINISHING ITEMS

S.No.	Item	Periodicity				
		Res. Bldg.	Office Bldg.	Hospitals	Laboratories	Schools
1	2	3	4	5	6	7
	White Washing/Colour washing	2 Years	2 Years	2 Years	2 Years	2 Years
2	Applying dry distemper	2 Years	2 Years	2 Years	2 Years	2 Years
3	Painting with plaster paint, Synthetic enamel paint, Oil bound distemper, acrylic paint, acrylic distemper	3 Years	2 Years	1 Year- Corridor O.T. Rooms 2 Years- Other areas	2 Years	3 Years
4	Painting external surface with water proofing cement paint	3 Years	3 Years	3 Years	3 Years	3 Years
6	Cleaning and disinfecting of water storage/distribution tanks, water mains.	6 months	6 months	3 months	3 months	6 months
7	Cleaning of Manholes/Gully chambers/ inspection chambers and flushing of building sewers	I year	1 year	6 months	1 year	1 year
8	Cleaning of storm water drains	1 year	1 year	1 year	1 year	1 year
9	Painting steel water tanks ins1de with bitumastic paint.	2 years	2 years	1 year	2 years	2 years
10	Polishing wooden doors/ windows with sprit polish/ Polish/synthetic acrylic polish.	5 years	5 years	5 years	5 years	5 years
11	Text mat or poly mat based equivalent synthetic silicon based exterior paint.	5 years	5 years	5 years	5 years	5 years
12	Cleaning Electrical installations, fans etc.	1 year	1 year	1 year	1 year	1 year
13	Premix, Semi dense/dense Carpeting of roads.	5 years	5 years	5 years	5 years	5 years
14	Collection of water samples for physical, Chemical and Bacteriological analysis of water	6 months	6 months	3 months	6 months	6 months

SHIVAJI UNIVERSITY, KOLHAPUR.

IT Policies & Guidelines
(Release: Jan. 2014 Version 1.0)

Prepared by
Special Technical Committee,
Shivaji University,
Vidya Nagar, Kolhapur 416004.

Table of Contents

Shivaji University's IT Policy
(Release: Jan. 2014 Version 1.0)

Need for IT Policy

- Basically the University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. Realizing the importance of these services, SUK took initiative way back in 2000 and established basic network infrastructure in the academic complex of the university.

Over the last ten years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the university's academic environment.

Now, the university has about 2500 network connections covering more than twenty buildings across the campus and expected to reach 4000 connections very soon.

Internet Unit is the department that has been given the responsibility of running the university's intranet & Internet services.

Internet Unit is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the university.

SUK is getting its Internet bandwidth from BSNL. Total bandwidth availability from BSNL source is 20 Mbps (leased line). SUK has also got 1 Gbps connectivity under NKN Network of MHRD (NME-ICT) via BSNL.

While educational institutions are providing access to Internet to their faculty, students and staff, they face certain constraints:

- Limited Internet bandwidth.
- Limited infrastructure like computers, computer laboratories,
- Limited financial resources in which faculty, students and staff should be provided with the network facilities and
- Limited technical manpower needed for network management.

On one hand, resources are not easily available for expansion to accommodate the continuous rise in Internet needs, on the other hand uncontrolled, uninterrupted and free web access can give rise to activities that are neither related to Teaching/learning processes nor governance of the university.

At the outset, we need to recognize the problems related to uncontrolled surfing by the users:

- Prolonged or intermittent surfing, affecting quality of work
- Heavy downloads that lead to choking of available bandwidth

- Exposure to legal liability and cases of sexual harassment due to harmful and embarrassing content.
- Confidential information being made public.

.

With the extensive use of the Internet, network performance suffers in three ways:

When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.

When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.

☐ When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users who are on the high speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available.

Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service. Reducing Internet traffic is the answer.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network.

Apart from this, plenty of employee time is lost with a workstation being scanned and cleaned of the virus. Emails, unsafe downloads, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untold damage to information on the network.

They can slow down or even bring the network to a halt.

Containing a virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial.

Hence, in order to securing the network, Internet Unit has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users.

As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions.

Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies are a sign of due diligence; often necessary in the event of an IT audit or litigation.

Policies also serve as blueprints that help the institution implement security measures.

An effective security policy is as necessary to a good information security program as a solid foundation to the building.

Hence, Shivaji University also is proposing to have its own IT Policy that works as guidelines for using the university's computing facilities including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information

Technology (IT)". Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this university.

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users.

Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations.

Guidelines are created and provided to help organisation, departments and individuals who are part of university community to understand how University policy applies to some of the significant areas and to bring conformance with stated policies.

IT policies may be classified into following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Web Site Hosting Policy
- University Database Use Policy

Further, the policies will be applicable at two levels :

- End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
- Network Administrators

It may be noted that university IT Policy applies to technology administered by the university centrally or by the individual departments, to information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by authorised resident or non-resident visitors on their own hardware connected to the university network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the university recognised Associations/Unions, or hostels and guest houses, or residences wherever the network facility was provided by the university.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the university IT policy.

Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the University's information technology infrastructure , must comply with the Guidelines. Certain violations of IT policy laid down by the university by any university member may even result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus
- Students: UG, PG, Research
- Employees   (Permanent/ Temporary/ Contractual)
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

Resources

- Network Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Mobile/ Desktop / server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

IT Hardware Installation Policy

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

A. **Who is Primary User**

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. **What are End User Computer Systems**

Apart from the client PCs used by the users, the university will consider servers not directly administered by INTERNET UNIT, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the INTERNET UNIT, are still considered under this policy as "end-users" computers.

C. **Warranty & Annual Maintenance Contract**

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.

D. **Power Connection to Computers and Peripherals**

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS

is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

E. **Network Cable Connection**

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

F. **File and Print Sharing Facilities**

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

G. **Shifting Computer from One Location to another**

Computer system may be moved from one location to another with prior written intimation to the INTERNET UNIT, as INTERNET UNIT maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation (from the list maintained by INTERNET UNIT) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified . When the end user meets the compliance and informs INTERNET UNIT in writing/by email, connection will be restored.

H. **Maintenance of Computer Systems provided by the University**

For all the computers that were purchased by the university centrally and distributed by the Estate Branch, University Computer Maintenance Cell (COMPUTER CENTER) will attend the complaints related to any maintenance related problems.

I. Noncompliance

SUK faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

J. INTERNET UNIT/COMPUTER CENTER Interface

INTERNET UNIT upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance.

Software Installation and Licensing Policy

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

2. University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

3. Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users responsibility to make sure that the updates a being done properly.

B. Antivirus Software and its updating

1. Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

C. Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a

foolproof solution. Apart from this, users should keep their valuable data either on Floppy, or CD or other storage devices such as pen drives.

D. Noncompliance

SUK faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons

An individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

E. INTERNET UNIT/COMPUTER CENTER Interface

INTERNET UNIT upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The Communication & Information Services (INTERNET UNIT) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to INTERNET UNIT.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the INTERNET UNIT. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorisedly from any other location.

As and when a new computer is installed in any location, the concerned user can download the application form available for the purpose of IP address allocation and fill it up and get the IP address from the INTERNET UNIT.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

B. DHCP and Proxy Configuration by Individual Departments /Sections/ Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by INTERNET UNIT.

Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

C. Running Network Services on the Servers

Individual departments/individuals connecting to the university network over the

LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the INTERNET UNIT in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.

INTERNET UNIT takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.

INTERNET UNIT will be constrained to disconnect client machines where potentially damaging software is found to exist.

A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes.

Network traffic will be monitored for security and for performance reasons at INTERNET UNIT.

Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

D. Dial-up/Broadband Connections

Computer systems that are part of the University's campus-wide network, whether university's property or personal property, should not be used for dial-up/broadband connections, as it violates the university's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

E. Wireless Local Area Networks

1. This policy applies, in its entirety, to School, department, or division wireless local area networks. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with INTERNET UNIT including Point of Contact information.

2. School, departments, or divisions must inform INTERNET UNIT for the use of radio spectrum , prior to implementation of wireless local area networks.

3. School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.

4. If individual School wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the university authorities whose application may be routed through the Co-ordinator, INTERNET UNIT.

F. Internet Bandwidth obtained by Other Departments

Internet bandwidth acquired by any Section, department of the university under any research programme/project should ideally be pooled with the university's Internet bandwidth, and be treated as university's common resource.

Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such network should be totally separated from the university's campus network. All the computer systems using that network should have separate

IP address scheme (private as well as public) and the university gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to INTERNET UNIT.

Non-compliance to this policy will be direct violation of the university's IT security policy.

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to **http://mail.unishivaji.ac.in** with their User **ID** and **password**. For obtaining the university's email account, user may contact INTERNET UNIT for email account and default password by submitting an application in a prescribed proforma.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. the facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. while sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
6. Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.
7. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

10. Impersonating email account of others will be taken as a serious offence under the university IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.
12. Any Spam mail received by the user into INBOX should be forwarded to spam@mail.unishivaji.ac.in
13. Any mail wrongly stamped as SPAM mail should be forwarded to wrongspam@mail.unishivaji.ac.in
14. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may forward that mail ID to netadmin@unishivaji.ac.in for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.

The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

Web Site Hosting Policy

1. Official Pages

Sections, departments, and Associations of Teachers/Employees/Students may have pages on SUK's Intranet Channel of the official Web page.

Official Web pages must conform to the University Web Site Creation Guidelines for Web site hosting.

As on date, the university's webmaster is responsible for maintaining the official web site of the university viz., http://www.unishivaji.ac.in only.

Personal Pages:

The university computer and network infrastructure is a limited resource owned by the university. It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the university by sending a written request to INTERNET UNIT giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the university. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups.

Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the university.

Affiliated Pages:

Faculty may host Web pages for "affiliated" professional organizations on department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

2. Web Pages for eLearning

Though the university does not have this facility as on this date, this Policy relates to future requirements for Web pages for eLearning authored as a result of Teaching/Learning process.

Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

Because majority of student pages will be published on the University's Web for eLearning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official SUK or other Web sites. If a student publishes a fictional Web site or a Web site modeled after an existing institution or corporation, the site must be clearly identified as a class project.

The following are the storage and content requirements for class-generated student Web pages:

Servers:

It is recommended that pages be placed on the student information server, but pages developed for classes also may be placed on departmental servers or the main campus server meant for eLearning purpose.

Maintenance:

If the pages are published on the eLearning information server, they will be maintained under the default rules for personal eLearning pages

The instructor will maintain pages that are published on departmental servers or the main campus server meant for eLearning purpose.

Content Disclaimer:

The home page of every class-generated site will include the SUK Content

Disclaimer (for pages published on the eLearning information server, the content disclaimer should be generated automatically):

Class Information:

The home page of every class-generated site will contain the name of the class, the student's name, the date, and a link to the class home page.

Pages Generated by Class Groups:

Pages produced by class groups, if placed on the eLearning information server, will be placed on the server under the name of the designated group leader.

Official Pages:

If Web pages developed for eLearning become the part of the "official" SUK page, they must be removed from the eLearning information server, departmental servers as class-generated pages (students, can of course, link to their work from their personal student pages).

3. Student Web Pages

Though the university does not have this facility as on this date, this policy relates to future requirements for personal student Web pages. Policies for student pages authored as a result of academic assignments are in II above. It is recognized that each individual student will have individual requirements for his/her pages. As the university's computer and network infrastructure is a limited resource owned by the university, only web pages of students related to their assignments will be accepted on the Students web pages. The contents of personal pages hosted by the students even on outside web site must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws.

The following are the storage and content requirements for personal student Web pages:

Servers:

Pages will be placed on the student information server.

Maintenance:

Pages published on the student information server will be maintained under the default rules for personal student pages.

Content Disclaimer:

Every personal page will include the SUK Content Disclaimer (the content disclaimer will be generated automatically):

Responsibilities for Those Maintaining Web Pages

Sections, departments, units, and individuals are responsible for maintaining their own Web pages.

SUK Web pages (including personal pages) must adhere to the SUK Web Page

Standards and Design Guidelines and should be approved SUK WebPages Advisory Committee.

Policies for Maintaining Web Pages

Pages must relate to the University's mission.

Authors of official SUK and affiliated pages (not class-generated or personal) are required to announce their Web presence by sending an announcement to

webmaster@unishivaji.ac.in. Mails sent to this address will be placed in a SUK Public E-Mail Folder in the SUK's official web site.. The announcement should include:

1. The URL.

2. A brief explanation of content or purpose of the pages (i.e., Web pages for an administrative or academic unit, etc.). The primary page must include a link to the SUK Home Page and, if applicable, contain additional links to the sponsoring organization or department.

University Database(of eGovernance) Use Policy

This Policy relates to the databases maintained by the university administration under the university's eGovernance.

Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential.

SUK has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this university resource.

A. **Database Ownership:** Shivaji University is the data owner of all the University's institutional data generated in the university.

B. **Custodians of Data:** Individual Sections or departments generate portions of data that constitute University's database. They may have custodianship responsibilities for portions of that data.

C. **Data Administrators:** Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

D. **MIS Components:** For the purpose of eGovernance, Management Information System requirements of the university may broadly be divided into seven categories. These are:

- MANPOWER INFORMATION MANAGEMENT SYSTEM (MIMS)
- STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)
- FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)
- PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (PRIMS)
- PROJECT INFORMATION MONITORING SYSTEM (PIMS)
- LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)
- DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYSTEM (DMIRS)

Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

1. The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.
2. Data from the University's Database including data collected by departments or individual faculty and staff, is for internal university purposes only.
3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies the university makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the University Registrar.
5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the University and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the University Registrar for response.
6. At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes.

This includes organizations and companies which may be acting as agents for the university or its departments.

7. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar, Director BCUD, Controller of Examinations and Finance officer of the University.

8. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

9. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to :

   - Modifying/deleting the data items or software components by using illegal access methods.
   - Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
   - Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
   - Trying to break security of the Database servers.

Such data tampering actions by university member or outside members will result in disciplinary action against the offender by the university authorities.

If the matter involves illegal action, law enforcement agencies may become involved.

RESPONSIBILITIES OF INTERNET UNIT

A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by INTERNET UNIT.
2. INTERNET UNIT operates the campus network backbone such that service levels are maintained as required by the University Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings' Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of INTERNET UNIT.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of INTERNET UNIT. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings will be decided by the INTERNET UNIT. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of INTERNET UNIT.
3. INTERNET UNIT will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
4. It is not the policy of the University to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the University's Internet links.

C. Network Expansion

Major network expansion is also the responsibility of INTERNET UNIT. Every 3 to 5 years, INTERNET UNIT reviews the existing networking facilities, and need for possible expansion. Network expansion will be carried out by INTERNET UNIT when the university makes the necessary funds available.

D. Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations INTERNET UNIT considers providing network connection through wireless connectivity.
2. INTERNET UNIT is authorized to consider the applications of Sections, departments, or divisions for the use of radio spectrum from INTERNET UNIT prior to implementation of wireless local area networks.
3. INTERNET UNIT is authorized to restrict network access to the Sections, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.

.

E. Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

F. Global Naming & IP Addressing

INTERNET UNIT is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. INTERNET UNIT monitors the network to ensure that such services are used properly.

G. Providing Net Access IDs and email Accounts

INTERNET UNIT provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the university upon receiving the requests from the individuals on prescribed proforma.

H. Network Operation Center

INTERNET UNIT is responsible for the operation of a centralized Network Operation Control Center. The campus network and Internet facilities are available 24 hours a day, 7 days a week. All network failures and excess utilization are reported to the INTERNET UNIT technical staff for problem resolution .

Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the INTERNET UNIT. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, INTERNET UNIT will analyse the net traffic offending actions or equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if need be, a report will be sent to higher authorities in case the offences are of very serious nature.

I. Network Policy and Technology Standards Implementation

INTERNET UNIT is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

J. Receiving Complaints

INTERNET UNIT may receive complaints from COMPUTER CENTER, if any of the network related problems are noticed by them during the course of attending the end-user computer systems related complaints. Such complaints should be by email/phone.

INTERNET UNIT may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone call to INTERNET UNIT.

The designated person in INTERNET UNIT receives complaints from the users/COMPUTER CENTER and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service

INTERNET UNIT will be responsible only for solving the network related problems or services related to the network.

L. Disconnect Authorization

INTERNET UNIT will be constrained to disconnect any Section, department, or division from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Section, department, or division machine or network, INTERNET UNIT endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Section, department, or division is disconnected, INTERNET UNIT provides the conditions that must be met to be reconnected.

Responsibilities of University Computer Center
A. Maintenance of Computer Hardware & Peripherals
COMPUTER CENTER is responsible for maintenance of the university owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

B. Receiving Complaints
COMPUTER CENTER may receive complaints from INTERNET UNIT, if any of the particular computer systems are causing network related problems.

COMPUTER CENTER may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in COMPUTER CENTER receives complaints from the users/INTERNET UNIT of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

C. Scope of Service
COMPUTER CENTER will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was loaded by the company.

D. Installation of Un-authorised Software
COMPUTER CENTER or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

E. Reporting IT Policy Violation Incidents
If COMPUTER CENTER or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the university, such incidents should be brought to the notice of the INTERNET UNIT and university authorities.

F. Reporting incidents related to Network Operations
When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the COMPUTER CENTER by INTERNET UNIT. After taking necessary corrective action COMPUTER CENTER or service engineers should inform INTERNET UNIT about the same, so that the port can be turned on by them.

G. Rebuilding the Computer System
When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net.

Further, before reformatting the hard disk, dump of only the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

H. Coordination with INTERNET UNIT
Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network or the software installed or hardware malfunctioning,

COMPUTER CENTER/service engineer may coordinate with INTERNET UNIT staff to resolve the problem with joint effort. This task should not be left to the individual user.

Responsibilities of Department or Sections

A. User Account

Any Centre, department, or Section or other entity can connect to the University network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the university. The user account will be provided by INTERNET UNIT, upon filling up the prescribed application form and submitting it to INTERNET UNIT.

Once a user account is allocated for accessing the university's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the university for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access Id and for email account ID) to prevent un-authorised use of their user account by others.

As a member of Shivaji University community, when using the university' network facilities and its user account, it becomes user's duty to respect the University's reputation in all his/her electronic dealings within as well as outside the University.

It is the duty of the user to know the IT policy of the university and follow the guidelines to make proper use of the university's technology and information resources.

B. Logical Demarcation of Department/ Section/Division Networks

In some cases, Section, department or Division might have created a internal network with in their premises. In such cases, the Section, department, or division assumes responsibility for the network service that is provided on all such internal networks on the School, department or division side of the network backbone. The School, department, or division is also responsible for operating the networks on their side of the network backbone

in a manner that does not negatively impact other network segments that are connected to the network backbone.

Each Section, department, or division should identify at least one person as a Point of Contact and communicate it to INTERNET UNIT and COMPUTER CENTER so that INTERNET UNIT or COMPUTER CENTER can communicate with them directly in case of any network/system related problem at its end.

C. Supply of Information by Section, Department, or
Division for Publishing on /updating the SUK Web Site

All Schools/Centers, Departments, or Divisions should provide updated information concerning them periodically (at least once in a month or earlier).

Hardcopy of such information duly signed by the competent authority at Section, Department, or Division level, along with a softcopy to be sent to the webmaster operating from INTERNET UNIT. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Section, Department, or Division.

Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the webmaster upon receiving the written requests. If such web pages have to be directly added into the official web site of the university, necessary content pages (and images, if any) have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format. Further, such requests along with the soft copy of the contents should be forwarded to the Director, INTERNET UNIT well in advance.

D. Setting up of Wireless Local Area Networks/Broadband Connectivity

1. This policy applies, in its entirety, to school, department, or division wireless local area networks/broadband connectivity within the academic complex. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with INTERNET UNIT including Point of Contact information.
2. Obtaining Broadband connections and using the computers alternatively on the broadband and the university campus-wide network is direct violation of the university's IT Policy, as university. IT Policy does not allow broadband connections within the academic complex.
3. School, departments, or divisions must secure permission for the use of radio spectrum from INTERNET UNIT prior to implementation of wireless local area networks.
4. School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.
5. As inter-building wireless networks are also governed by the University IT Policy, setting up of such wireless .networks should not be undertaken by the Schools/Centers without prior information to INTERNET UNIT.

E. Security

In connecting to the network backbone, a school, department, or division agrees to abide by this Network Usage Policy under the University IT Security Policy. Any network security incidents are resolved by coordination with a Point of Contact (POC) in the originating department. If a POC is not available to contact, the security incident is resolved by disconnecting the offending computer from the network till the compliance is met by the user/POC.

F. Preservation of Network Equipment and Accessories

Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the university are the property of the university and are maintained by INTERNET UNIT.

Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to,

*   Removal of network inlet box.
*   Removal of UTP cable from the room.
*   Opening the rack and changing the connections of the ports either at jack panel level or switch level.
*   Taking away the UPS or batteries from the switch room.
*   Disturbing the existing network infrastructure as a part of renovation of the location INTERNET UNIT will not take any responsibility of getting them rectified and such tampering may result in disconnection of the network to that segment or the individual, until the compliance is met.

G. Additions to the Existing Network

Any addition to the existing network done by Section, department or individual user should strictly adhere to the university network policy and with prior permission from the competent authority and information to INTERNET UNIT.

University Network policy requires following procedures to be followed for any network expansions:

- All the internal network cabling should be as on date of CAT 6 UTP.
- UTP cabling should follow structured cabling standards. No loose and dangling UTP cables be drawn to connect to the network.
- UTP cables should be properly terminated at both ends following the structured cabling standards.
- Only managed switches should be used. Such management module should be web enabled. Using unmanaged switches is prohibited under university's IT policy. Managed switches give the facility of managing them through web so that INTERNET UNIT can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.
- As managed switches require IP address allocation, the same can be obtained from INTERNET UNIT on request.

H. Structured Cabling as a part of New Buildings

All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans like any other wiring such as electrical and telephone cabling, for LAN as a part of the building layout Plan. Engineering Branch may make provisions in their designs for at least one network point in each room. All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

I. Campus Network Services Use Agreement

The "Campus Network Services Use Agreement" should be read by all members of the university who seek network access through the university campus network backbone. This can be found on the Intranet Channel of the university web site. All provisions of this policy are considered to be a part of the Agreement. Any Section, Department or Division or individual who is using the campus network facility , is considered to be accepting the university IT policy. It is user's responsibility to be aware of the University IT policy. Ignorance of existence of university IT policy is not an excuse for any user's infractions.

J. Enforcement

INTERNET UNIT periodically scans the University network for provisos set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines.

Responsibilities of the Administrative Units

INTERNET UNIT needs latest information from the different Administrative Units of the University for providing network and other IT facilities to the new members of the university and for withdrawal of these facilities from those who are leaving the university, and also for keeping the SUK web site up-to-date in respect of its contents.

The information that is required could be broadly of the following nature:

- Information about New Appointments/Promotions.
- Information about Super annuations / Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Any action by the university authorities that makes n individual ineligible for using the university's network facilities.
- Information on Important Events/Developments/Achievements.
- Information on different Rules, Procedures, Facilities Information related items nos. A through E should reach Director (INTERNET UNIT) and Information related items nos. F and G should reach webmaster well in-time.

Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy (either on mobile storage devices or mobiles or PDA or by email) should be sent to INTERNET UNIT so as to reach the above designated persons.

Guidelines on Computer Naming Conventions

1. In order to troubleshoot network problems and provide timely service, it is vital to be able to quickly identify computers that are on the campus network. All computer names on the campus network must use the University standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of INTERNET UNIT.

2. All the computers should follow the standard naming convention

Guidelines for running Application or Information Servers

Running Application or Information Servers

i Section/Departments may run an application or information server.

ii Individual faculty, staff or students on the SUK campus may not run personal, publicly available application or information servers (including content or services providing programs such as ftp, chat, news, games, mail, ISP, etc.) on the SUK network.

Responsibilities for Those Running Application or Information Servers

Sections/Departments may run an application or information server. They are responsible for maintaining their own servers.

1) Application or information server content and services must follow content guidelines as described in SUK Guidelines for Web Presence.

2) Obtain an IP address from INTERNET UNIT to be used on the server

3) Get the hostname of the server entered in the DNS server for IP Address resolution. University IT Policy's naming convention should be followed while giving the host names.

4) Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.

5) Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.

6) Operating System and the other security software should be periodically updated.

7) Sections/Departments may run an application or information server provided they do the following:

I. Provide their own computer, software and support staff

II. Provide prior information in writing to INTERNET UNIT on installing such Servers and obtain necessary IP address for this purpose.

For general information to help you decide whether or not to run a department or organization web server, contact the INTERNET UNIT.

Guidelines for hosting Web pages on the Internet/Intranet.

Mandatory:

1. Provide the full Internet e-mail address of the Web page maintainer.
2. Provide a link to the SUK home page from the parent (department of origin) home page.
3 Provide a link to the parent home page ("Return to department's home page") on all supporting local pages.
4. Maintain up to date pages. Proofread pages and test links before putting them on the Web, and regularly test and update links.
5. Know the function of HTML tags and use them appropriately.
6 Make provision for providing information without images as printer-friendly versions of the important web pages.

Recommended:

1. Provide information on timeliness (for example: August 2005; updated weekly; updated monthly, etc.)..
2 Provide a section indicating "What's New."
3. Provide a caution statement if link will lead to large pages or images.
4. Indicate restricted access where appropriate.
5. Avoid browser-specific terminology.
6. Provide link text that is clear without the link saying '**click here**' whenever hyperlinks are used.
7 Maintain visual consistency across related pages.
8. Provide a copyright statement (if and when appropriate).
9. Keep home pages short and simple.
10. Avoid using large graphics or too many graphics on a single page.
11. Provide navigational aids useful to your users (Link to Home, Table of
Contents, Next Page, etc.).
12. Maintain links to mentioned pages.
13. Make your Web pages easy to maintain for yourself and anyone who might maintain them in the future.
14. Avoid active links to pages that are in development. Place test or draft pages in your "test," "temp," or "old" subdirectory. Remember that nothing is private on the Internet: unlinked pages in your directory may be visible.
15 Check your finished page with a variety of browsers, monitors, and from both network and modem access points. It is also recommended that you check your page with a Web validation service.
16. Think of your users--test with primary user groups (which will be mix of users linking through our high-speed network, and users linking via much slower modems).
17 Conform to accepted, standard HTML codes.

Guidelines for Desktop Users

These guidelines are meant for all members of the SUK Network User Community and users of the University network.

Due to the increase in hacker activity on campus, University IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

1. All desktop computers should have the latest version of antivirus such as Symantec Anti Virus (PC) or Quick Heal and should retain the setting that schedules regular updates of virus definitions from the central server.

2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine.

Whenever possible, security policies should be set at the server level and applied to the desktop machines.

3. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.

4. The password should be difficult to break. Password, defined as:

i. must be minimum of 6-8 characters in length

ii. must include punctuation such as ! $ % & * , . ? + - =

iii. must start and end with letters

iv. must not include the characters # @ ' " `

v. must be new, not used before

vi. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.

vii. passwords should be changed periodically and also when suspected that it is known to others.

viii. Never use 'NOPASS' as your password

ix. Do not leave password blank and

x. Make it a point to change default passwords given by the software at the time of installation

5. The password for the user login should follow the same parameters outlined above.

6. The guest account should be disabled.

7. New machines with Windows XP should activate the built-in firewall.

8. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.

9. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks).

When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

10. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

11. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.

12. In addition to the above suggestions, INTERNET UNIT recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise.

Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

13. If a machine is compromised, INTERNET UNIT will shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.

14. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, INTERNET UNIT technical personnel can scan the servers for vulnerabilities upon request.

Video Surveillance Policy

The system

1.1   *The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.*

1.2   *Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.*

1.3   *Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Cemera installation is in use.*

1.4   Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

2.0   Purpose of the system

2.1   The system has been installed by university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

2.2   Covert recording

2.2.1   Covert cameras may be used under the following circumstances on the written authorisation or request of the Senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

2.2.2   Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

2.2.3   The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

3.0   The Security Control Room

3.1   Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

3.2   No unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry..

3.3   Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorisation from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.

3.4   Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organisation they represent, the person who granted authorisation and the times of entry to and exit from the centre. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

4.0   Security Control Room Administration and Procedures

4.1   Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

4.2   Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

5.0   Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Cemera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Cemera.

6.0   Recording

6.1   Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

6.2   Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

6.3   All hard drives and recorders shall remain the property of university until disposal and destruction.

7.0   Access to images

7.1   All access to images will be recorded in the Access Log as specified in the Procedures Manual

7.2   Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

7.3.0   Access to images by third parties

7.3.1   Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

7.4.0 Access to images by a subject

CCTV/IP Cemera digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by C.C.T.V. /IP Cemera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

7.4.1 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms are obtainable from the Security Office, between the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except Second and fourth Saturday), except when university is officially closed or from the Data Protection Officer, the Records Office during the same hours.

7.4.2 The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the university Data Protection Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.

7.4.3 The Data Protection Act gives the Data Protection Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

7.4.4 All such requests will be referred to the Security Control room Supervisor or by the Data Protection Officer.

7.4.5 If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

8.0 Request to prevent processing

8.1 An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

8.2 All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Data Protection Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

9.0 Complaints

9.1 It is recognised that members of University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralised Complaints Procedure by

obtaining and completing a University Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer, These rights do not alter the existing rights of members of University or others under any relevant grievance or disciplinary procedures.

10.0   Compliance monitoring

10.1   The contact point for members of University or members of the public wishing to enquire about the system will be the Security Office which will be available during the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except second and fourth Saturday) except when University is officially closed.

10.2   Upon request enquirers will be provided with:

A summary of this statement of policy

An access request form if required or requested

A subject access request form if required or requested

A copy of the University central complaints procedures

10.3   All documented procedures will be kept under review and a report periodically made to the Estates Management Committee.

 10.4   The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Estates Management Committee.

<div align="center">

Appendix I
Campus Network Services Use Agreement
</div>

Read the following important policies before applying for the user account/email account. By signing the application form for IP address allocation/Net Access ID(user account)/email account , you agree to act in accordance with the IT policies and guidelines of Shivaji University. Failure to comply with these policies may result in the termination of your account/IP address. It is only a summary of the important IT policies of the university. User can have a copy of the detailed document from the Intranet (viz.**http://www.SUK.ac.in/intranetchannel/SUK_ITpolicy.pdf**).

A Net Access ID is the combination of a username and a password whereby you gain access to University computer systems, services, campus networks, and the internet.

I. Accounts and Passwords

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. The User will not share the password or Net Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the University.

Students, staff and faculty who leave the University will have their Net Access ID and associated files deleted.

No User will be allowed more than one Net Access ID at a time, with the exception that faculty or officers who hold more than one portfolio, are entitled to have Net Access ID related to the functions of that portfolio.

II. Limitations on the use of resources

On behalf of the University, INTERNET UNIT reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

III. Computer Ethics and Etiquette

The User will not attempt to override or break the security of the University computers, networks, or machines/networks accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. Even sending unsolicited bulk e-mail messages comes under IT Policy violation.

In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

User's Net Access ID gives him/her access to e-mail, and campus computing resources. The use of these resources must comply with University policy and applicable. Electronically available information

(1) may not contain copyrighted material or software unless the permission of the copyright owner has been obtained,

(2) may not violate University policy prohibiting sexual harassment,

(3) may not be used for commercial purposes,

(4) should not appear to represent the University without appropriate permission, or to represent others,

(5) may not appear to represent other organizations or companies,

(6) may not contain material which violates pornography laws, or algorithms or software which if transferred violate laws,

(7) may not contain scripts or code that could cause a security breach or permit use of resources in opposition to University policy, and

(8) WWW pages should clearly show identifying information of the owner of the page and we suggest that it also show date of last revision and an address (e-mail or postal) for correspondence. INTERNET UNIT equipment does not support use of scripting in individual pages.

IV. **Data Backup, Security, and Disclaimer**

INTERNET UNIT or COMPUTER CENTER will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an

INTERNET UNIT/COMPUTER CENTER staff member in the process of helping the user in resolving their network/computer related problems. Although INTERNET UNIT/COMPUTER CENTER make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, INTERNET UNIT makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold INTERNET UNIT or COMPUTER CENTER, as part of SUK, harmless for any such liability or expenses. SUK retains the right to change and update these policies as required without notification to the User.

V. **Account Termination and Appeal Process**

Accounts on SUK network systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other inappropriate use of computing and network resources. When an account is terminated or disabled, INTERNET UNIT will make an attempt to contact the user (at the phone number they have on file with INTERNET UNIT) and notify them of the action and the reason for the action. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the INTERNET UNIT of the same But, if the termination of account is on the grounds of willful breach of IT policies of the university by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may first approach the Director INTERNET UNIT, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Appeals Board duly constituted by the university for this purpose to review the evidence and hear reasons why an appeal should be considered. If the Appeals Board recommends revival of the account, it will be enabled. However, the Internet Unit of the Appeals Board is final and should not be contested.

Users may note that the University's Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate University authorities.

SHIVAJI UNIVERSITY, KOLHAPUR.
INTERNET UNIT
Application for IP Address Allocation
S.No. Details To be filled

1. Location of the System Section / Department : _____

Room No. _____

Floor /Lab.No _____

Occupied by _____

2. Identification Name of the System
(Hostname)

_____

3. IO Box Number _____

4.. Make of the system ACER / Compaq / HCL / IBM / HP / Dell / If Other, Specify

_____

5. MAC / Physical / Adapter address

6. Operating System Win95, Win98, W2K, WinXP, Linux, Solaris, if Other, specify _____

7. Net-based Applications Running on the
system
a. Yahoo Messenger
b. MSN Messenger
c. AOL
d. Microsoft Antispyware
e. SPSS
f. Others, specify…………………………………………..

8 Whether connected directly to the LAN or through another hub / switch
YES / NO, If yes ,
a. Directly connected to LAN
b. Through Hub/Switch located in the same room / different room

9. If the system is configured as server , services that are enabled
a. Http h. SMTP
b. FTP i. Sendmail
c. Netfs j. MySql
d. Network k. SMB
e. Nfs l. Telnet

f. POP3, m. **Any other ,specify_____**
g. IMAP,

10. Whether in general used by single user or many users
Single / Many

11. Which Antivirus Software is running _____

Date:

Signature of the Applicant

INTERNET UNIT Office Use only
IP address allocated by INTERNET UNIT

Applicant's copy
Signature on Behalf of Co-ordinator, INTERNET UNIT

SHIVAJI UNIVERSITY, KOLHAPUR.
INTERNET UNIT
Application for Net Access ID Allocation

Date:

Signature of the Applicant

INTERNET UNIT Office Use only

Net Access ID allocated by INTERNET UNIT

Applicant's copy

Signature

on Behalf of Co-ordinator, INTERNET UNIT

S.No. Details To be filled

1. Name of the Applicant Prof./Dr./Mr./Ms./ ……………………………………….

2. Location Section / Department :

Room No. _____

Contact Telephone No. _____

3. Date of birth ----/----/------

4. Designation _____

5. Whether the appointment is permanent? Yes/No

if No, appointment valid up to : Dt.: / /

Net Access

ID allocated

Name of account holder

Account

Valid Up to

Net Access

ID allocated

Name of account holder

Account

Valid Up to

SHIVAJI UNIVERSITY, KOLHAPUR.

INTERNET UNIT

Application for WiFi Network Access Account Allocation for Students.

Date:

Mr./Ms…………………………... is a bonafide student of this department and the information given above by him/her is correct as per our records. He/she may be given WiFi Net Access.

Applicant's copy

Details to be filled

1. Name of the Applicant Mr./Ms.………………………………….

2. Department Name :　_____

3. Roll No. / Seat No. / PRN　_____

4. Course Name _____

5. Duration of the course __ Semesters

6. Date of joining the Course __/__/_____

7. Net Access device : Laptop / Mobile / Tablet

8. MAC address (Please get help of Internet Unit, if you cannot find)

Signature of the Applicant.

Signature and seal of Head of the Department

INTERNET UNIT Office Use only

MAC id verified:

Network Access ID allocated by INTERNET UNIT

Net Access ID allocated   YSE / NO

Account Valid Up to :   /   / 2014 to   /   / 2015

Co-ordinator, Internet Unit.

IT POLICY – SUK   42

SHIVAJI UNIVERSITY, KOLHAPUR.
INTERNET UNIT
REQUISITION FORM FOR E-MAIL ACCOUNT

1. Full Name : _____

2. Designation : _____

3. Dept./School
/Centre : _____

4. Office Telephone :_____

5. Please specify the E-mail Account Name you wish to have

Option One

@mail.unishivaji.ac.in

Option two

@mail.unishivaji.ac.in

Date : Signature of the Applicant

User Counterfoil

The following email ID is created for Prof./Dr./Mr./Ms _____

_____

on _____.

@mail.unishivaji.ac.in

Signature on Behalf of Co-ordinator, INTERNET UNIT

Appendix VI
SHIVAJI UNIVERSITY, KOLHAPUR.
INTERNET UNIT
REQUISITION FORM FOR STUDENTS' E-MAIL ACCOUNT

(USE BLOCK LETTERS ONLY)

1. Full Name : _____

2. Programme of Study : _____

3. School : __ _____

4. Centre :____ _____

5. Year of Admission : _____

6. Semester : Monsoon/Winter

7. Permanent Address :

_____

_____

8. Local Address :

_____

_____

9. Telephone/Mobile No. if any: _____ _____

10. Identity Card No. : _____

Declaration

The above information furnished by me is correct, and I undertake to abide by the rules and regulations of the University for proper use of email facility for my research work purpose.

Date : **SIGNATURE OF THE STUDENT**

_____   _____

_____

Application for email account recommended by
Signature Signature & Stamp of
Supervisor Chairperson/ Dean
Counterfoil
Mr./Ms. _____
*Email Account :_____**@students.unishivaji.ac.in**
Signature
On behalf of Co-odinator

_____
* To be assigned by the INTERNET UNIT